A+

C o m p t i a

گردآورنده:
Payam Avarwand

مقدمه:

مدرک A+ شامل دو آزمون می باشد: 220-1001 و 220-1002
با توجه به فناوری روز و بکارگیری های متفاوت از آن، سوالات هریک از این دو آزمون، گاه به گاه به روز رسانی می شوند.

- از آنجایی که این کتاب، علیرغم تمرکز و دقت کافی بر مواد امتحانی هر دو آزمون، اما همه ی سرفصل های هردو آزمون را شامل نمی شود (مثل آشنایی مقدمانی با سیستم عامل Linux و آشنایی با مقدمات با امنیت)، پیشنهاد می شود قبل از آماده شدن برای هریک از آزمون ها، در سایت Comptia، سرفصل های امتحان موردنظر را مطالعه نمایید، تا از مباحث غایب در این کتابچه مطلع شده و آنها را جداگانه مطالعه کنید:

https://www.comptia.org/

- از طرف دیگر، اطلاع از پاسخ صحیح خیلی از سوالات در هردو آزمون A+، نیازمند **تجربیات کاری بسیار بالا** می باشد، که به سادگی در هیچ کتابی در مورد آنها صحبت نمی شود، و هرکسی نمی تواند همه ی این تجربیات را کسب کرده باشد!
به همین جهت، راهکار معقولانه تر این است که سوال های آخرین نسخه های آزمون موردنظر را از سایت های مرتبط با انتشار نمونه سوال، دریافت و مطالعه نمایید:

https://www.examtopics.com/
https://www.certbus.com/
...

- همانطور که مشاهده می کنید، این کتابچه دارای دسته بندی های منظم و سلسله مراتبی است که پس از باز کردن آن –مثلاً توسط نرم افزار Adobe Reader، با باز کردن تب Bookmarks، به سادگی به سرتیترهای این دسته بندی، دسترسی خواهید داشت که باعث سرعت عمل در کار با کتاب و دسترسی به موضوعات مختلف آن، خواهد بود.

1 Bit	0 | 1	
1 Byte	8 Bits	
128 Bytes	1 Kilo Bit	1024 Bits
1 Kilo Byte	1024 Bytes	8 Kilo Bits
1 Mega Byte	1024 Kilo Bytes	1,048,576 Bytes
1 Giga Byte	1024 Mega Bytes	1,073,741,824 Bytes
1 Tera Byte	1024 Giga Bytes	1,048,576 Mega Bytes
1 Peta Byte	1024 Tera Bytes	1,048,576 Giga Bytes
1 Exa Byte	1024 Peta Bytes	1,048,576 Tera Bytes

Practical Signs:

Sign	Name
/	Slash
\	Backslash
|	Pipe
,	Comma
:	Colon
;	semicolon
"	double quote
<	left angle bracket
>	right angle bracket
=	equals sign
&	Ampersand
≈	almost equal to
'	Apostrophe
*	Asterisk
@	At Sign
.	Bullet
^	Caret
✓	Checkmark
{	Curly Brackets
}	Left Curly Bracket
°	Degree
¨	Umlaut
÷	Division Sign
-	EN Dash
_	EM Dash
!	Exclamation Mark
♀	Female Sign
½	One half fraction
¼	One Quarter fraction
⅓	One third fraction
¾	Three quarters fraction
>	Greater Than Sign
∞	Infinity
<	Less Than Sign
♂	Male Sign
×	Multiplication Sign
#	Number Sign
Ω	Ohm Sign
(	Parenthese
)	Left Parenthesis
%	Percent Sign
£	Pound Sign
?	Question Mark
"	Quotation Marks
§	Section Sign
[	Square Brackets
]	Left Bracket

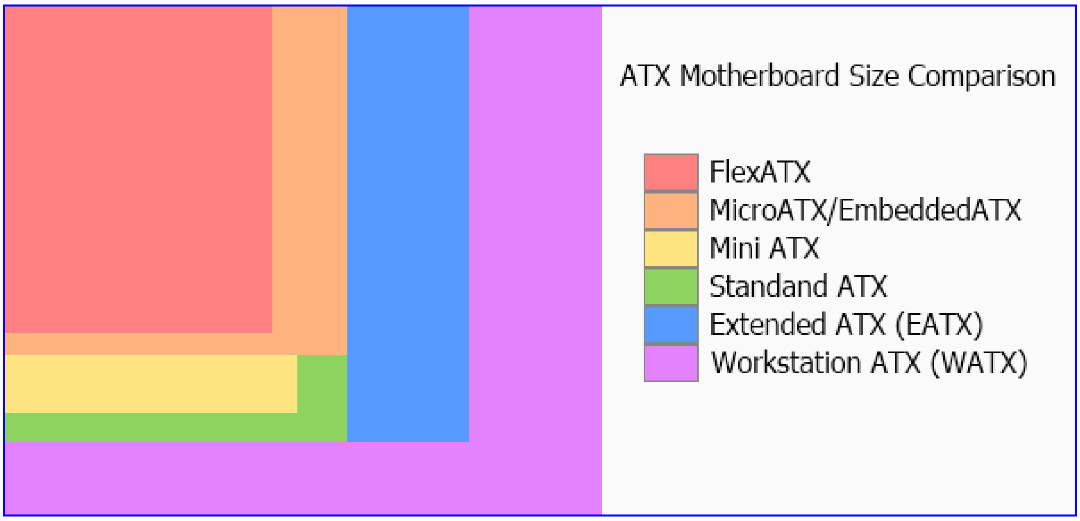
Case and Mother Board Dimensions :

در ابتدا، برای فضای داخلی Case های کامپیوتر، یک نوع Form Factor تعیین و ثبت کردند و آن را گسترش داده و انواع دیگری نیز طراحی و ثبت شدند.

از طرف دیگر، بر اساس Form Factor های کیس ها، Main board ها هم این Form Factor ها را پیروی کرده و مطابق با آنها، تولید شده و می شوند.

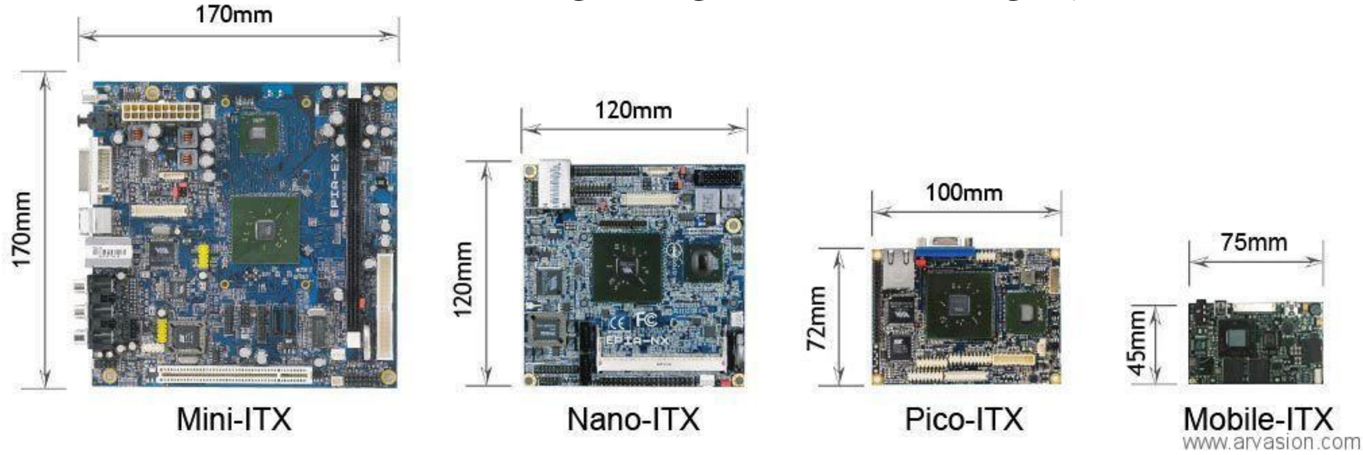
❖ ATX (Advanced Technology eXtended) :

- **Workstation-ATX و یا WTX :**
  - ابعاد آن تقریباً "16.75 × "14 و یا 35.5cm x 42.5cm می باشد.
- **Extended ATX و یا EATX:**
  - ابعاد : "12" x 13 و یا 30.4cm x 33cm
- **Standard ATX و یا Full ATX و یا ATX:**
  - ابعاد : "12" x 9.6 و یا 30cm x 24cm
- **Mini-ATX :**
  - ابعاد : "11.2" x 8.2 و یا 28cm x 21cm
  - مهم ترین تفاوت Mini با Full در تعداد Slot ها و درگاه های دیگر است.
  - کیسی که ATX باشد، قطعاً Mini-ATX را نیز پشتیبانی می کند.
- **Micro-ATX :**
  - ابعاد : "9.6" x 9.6 و یا 24cm x 24cm
  - کیسی که ATX باشد، Micro-ATX را نیز پشتیبانی می کند.
- **Flex-ATX :**
  - ابعاد : "9" x 7.5 و یا 22,9 cm x 19,1 cm

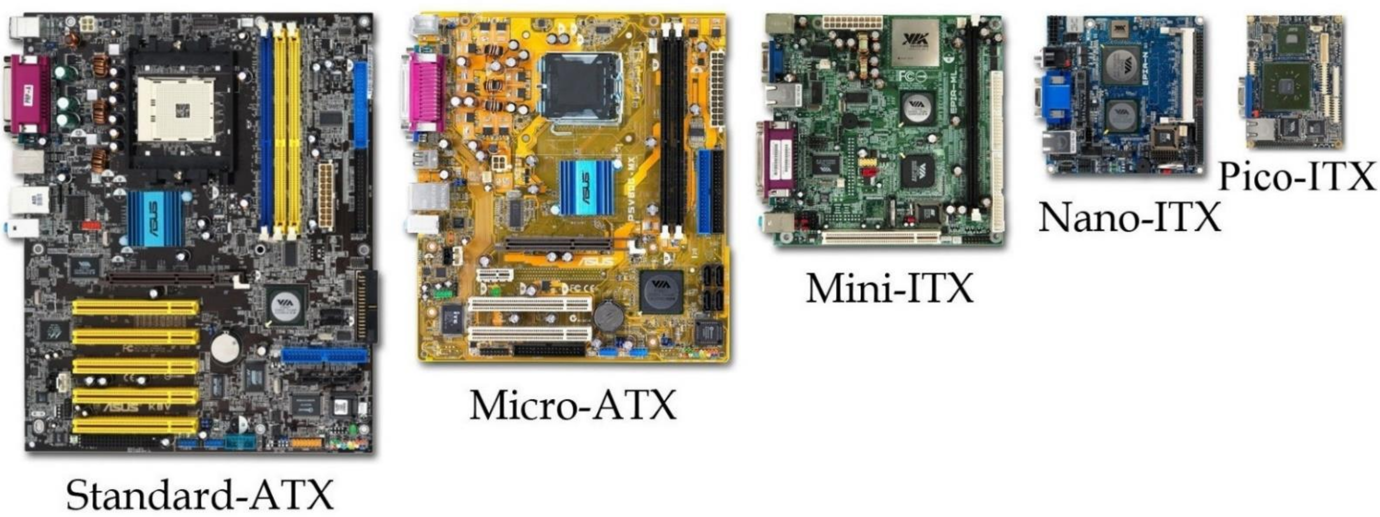


❖ ITX (Information Technology eXtended) :

- **Mini-ITX :**
  - ابعاد آن 17 cm x 17 cm و یا "6.75" x 6.75 می باشد.
  - مهم ترین ویژگی آن مصرف کم برق آن است.
  - جای تمام سوراخ های آن با ATX یکسان است.
- **Nano-ITX :**
  - ابعاد آن 12 cm x 12 cm و یا "4.7" x 4.7 می باشد.
- **Pico-ITX :**
  - ابعاد آن 7.2cm x 10cm و یا "2.8" x 3.9 می باشد.
- **Mobile-ITX :**
  - ابعاد آن 6 cm x 6 cm و یا "2.4" x 2.4 می باشد.
  - به جز یک پورت ورودی/خروجی، هیچ پورت دیگری ندارد.
  - بیشتر در پزشکی، حمل و نقل و کاربردهای نظامی استفاده می شود.



در زیر، رایج ترین Form Factor های ذکر شده، از لحاظ ظاهری، قابل مقایسه هستند.



➢ Case :

Case ها، از لحاظ فضای بیرونی، اغلب به شکل «ساختمان» ایستاده قرار می گیرند، از این جهت به آنها بُرج یا **Tower** نیز گفته می شود.
در شکل زیر **Tower** ها و کامپیوترهای کوچکتر را مشاهده می کنید.





:Internal Devices

:Mainboard

- وقتی یک **Mainboard** خریداری می کنیم، باید **Serial Number** ای که بر روی برچسب جعبه ی آن درج شده است، با **Serial Number** ای که بر روی کارت گارانتی درج شده است و همچنین با **Label** ای که روی خود **Mainboard** (معمولاً روی یکی از دیواره های **PCIe** و یا روی صفحه ی آن بصورت بزرگ) درج شده است، یکسان باشد.
- برای حفظ پشتیبانی **warranty** ابتدا آن را چک می کنیم که هیچ جای پیچ و یا هرگونه خراشی نداشته باشد، و سپس بدون اینکه **Mainboard** را نصب و پیچ کنیم، روی آن سیستم عامل نصب می کنیم و پس از اتمام نصب و راه اندازی سیستم عامل بر روی آن، آن را پیچ می کنیم.

➢ BIOS :

بایوس مخفف عبارت **Basic Input/Output System** بوده که سه نوع **AMI** و **AWARD** و **Phoenix** دارد و عبارت است از یک **Chip** الکترونیکی که با نام‌های زیر نیز شناخته می‌شود:

- **System BIOS**
- **ROM BIOS**
- **PC BIOS**

- تراشه ی **Bios** حاوی یک **Firmware** است.
- **BIOS** فقط خواندنی است، به همین دلیل به آن **ROM BIOS** نیز گفته می‌شود.
- حافظه های فقط خواندنی هم تحت شرایطی مانند **update** کردن، قابل تغییر هستند.
- ما **BIOS** را **Update** می کنیم تا **Feature** های جدید به آن افزوده شده و باگ های آن حذف شوند.
- این تراشه روی تمامی عناصر موجود در **Mainboard** مدیریت دارد و اطمینان از سالم بودن اجزای روی آن را می دهد.
- زمانی که کامپیوتر را روشن می‌کنید، **BIOS** وارد عمل شده و همان طور که از نامش پیداست، انواع خروجی‌ها و ورودی‌ها را تشخیص داده، مدیریت کرده و آن‌ها را تست می‌کند. پس از موفقیت آمیز بودن **test**، سیستم عامل را راه اندازی کند.
- راه اندازی سیستم عامل، با تشخیص دادن رکورد راه انداز اصلی (**MBR**) که روی حافظه تنظیم شده است، انجام می گیرد.
- برای ورود به تنظیمات **BIOS**، در کامپیوترهای **Client**، هنگام روشن شدن سیستم، **F11** یا **F12** را چندبار فشار می دهیم.

وظایف BIOS:

- **Power On Self Test (POST) : قطعات سخت افزاری را قبل از راه اندازی سیستم عامل تست و بررسی می‌کند تا از سالم بودن و کارکردن صحیح آن‌ها مطمئن شود. درصورت وجود مشکل در قطعات سخت افزاری (مثل نصب نبودن RAM) آن خطا توسط بوق‌هایی که به Beep معروف اند به کاربر اطلاع داده می‌شوند. مهمترین بوق های Bios :**

1. **یک بوق: زمانی که کامپیوتر روشن است اگر یک بوق بشنوید یعنی RAM (Random Access Memory) مشکل دارد یا مدار الکترونیکی مخصوص به آن و یا یکی از SLOT های مربوط به آن، مشکل پیدا کرده است.**
2. **دو بوق: باز هم به معنای ایراد در RAM است، اما به اسم تست تطابق حافظه parity error شناخته شده می شود که باید با نصب درست RAM در Slot، مشکل را برطرف کنیم.**
3. **سه بوق: باز هم باید RAM را در آورده و دوباره وصل کنیم، اما اگر تکرار شد، باید جایگزین کنیم.**
4. **چهار بوق: در Timer مادربرد خطائی پیش آمده و باید عوض کنید.**
5. **پنج بوق: به خطایی در CPU یا Mainboard دلالت دارد که احتمالاً باید آن را عوض کنیم.**
6. **شش بوق: دلالت بر خطا در Mainboard دارد که در واقع آسیب دیده و احتمال هم دارد که درست نصب نشده باشد و اگر بعد از نصب صحیح مشکل رفع نشد، باید Mainboard جدید جایگزین شود.**
7. **هشت بوق: مشکل در کارت گرافیک یا حافظه ی آن است که باید آن را جدا و مکان آن را پاک کرده و دوباره نصب کنیم و اگر مشکل ادامه داشت، باید جایگزین شود.**
8. **نه بوق: دلالت بر خطا در Bios دارد که باید update شود یا خود آن را تعویض کنیم، اما از همان نوع و سازگار با کامپیوتر!**

- **بنا بر نیاز کاربر، تطابق و هماهنگی قطعات، کارایی و عملکرد سیستم و تنظیمات پایه‌ای سخت افزارها را بررسی می کند.**
- **آخرین و مهمترین وظیفه ی بایوس این است که کنترل سیستم را به سیستم عامل می‌سپارد.**

برای این کار، به ترتیب حافظه‌هایی که برای Boot شدن، اولویت بندی شده‌اند را چک کرده و درصورتی که همه چیز Ok باشد، سیستم عامل را بارگذاری می‌کند.

- **در مادربرد های قدیمی BIOS در حافظه ROM و بر روی Mainboard قرار داشت.**

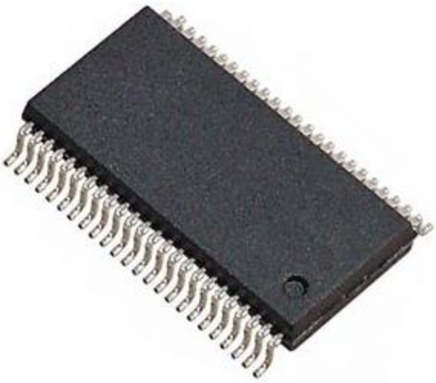
در مادربردهای جدیدتر، BIOS در حافظه ی Flash، اما همچنان در ROM قرار دارد.

- **قرار گرفتن BIOS در حافظه ی Flash این امکان را فراهم می کند تا راحت تر بتوان BIOS را Update کرد.**

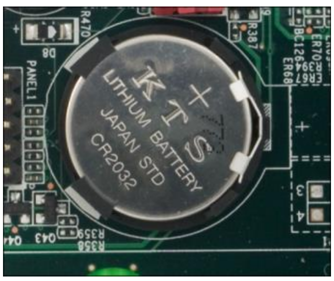
➢ CMOS Memory :

کار دیگری که BIOS باید انجام دهد، ذخیره کردن تنظیماتی است که کاربر در صفحه ی رابط کاربری BIOS انجام می دهد تا در زمانی که کامپیوتر خاموش است این تنظیمات حفظ شوند.

BIOS این تنظیمات را در CMOS Memory نگهداری می کند.



- **حافظه ی CMOS یک حافظه ی دائم با ظرفیتی محدود است.**
- **علاوه بر مشخصات BIOS، اطلاعات دیگری مثل ساعت و تاریخ رایانه را نیز در خود ذخیره می کند.**
- **CMOS Memory انرژی خود را از طریق باتری که روی Mainboard نصب می شود، تامین می کند.**



➢ Cache :

- حافظه ی پنهان یا Cache Memory ، حافظه ای کوچک و بسیار سریع است که قیمت بالایی هم دارد و در کنارCPU قرار دارد.
- Cache برای جلوگیری از تأخیر زمانی در دسترسی به اطلاعات مورد نیاز CPU بکار می رود.
- وقتی CPU چند بار به اطلاعاتی نیاز داشته باشد، پس از اولین دریافت، آنها را در حافظه ی کش قرار می دهد که در کنار دستش است، و دیگر به RAM بر نمی گرداند تا زمانی که کارش با آن اطلاعات کاملاً تمام شود. به این روش، Caching گفته می شود.
- Cache Memory از نوع SRAM است: Static Random Access Memory ، یعنی حافظه ی با دسترسی تصادفی ثابت. در حالی که قطعه ی کارت مانند RAM در کامپیوتر، از نوع DRAM است، یعنی Dynamic Random Access Memory .

➢ Firmware :

- در واقع می توان از Firmware به عنوان ترکیبی از نرم افزار و سخت افزار یاد کرد.
- Firmware ترکیبی از کدهای برنامه در حافظه ی دائمی سیستم یا ROM (Read Only Memory) و داده هایی است که درون آن ذخیره شده اند.
- شما در تجهیزاتی مثل مودم ها ، چراغ های راهنما ، کنترل تلوزیون ، ساعت های دیجیتال ، تجهیزات جانبی کامپیوتر و بسیاری از دوربین های عکاسی از Firmware استفاده می کنید. در واقع این Firmware است که امکان کنترل کردن دستگاه را برای شما میسر می کند.
- از آنجایی که رابط بین کاربر و سخت افزار، سیستم عامل نامیده می شود، Firmware را نیز می توان به عنوان یک سیستم عامل لایه پایین برشمرد.
- اما نکته اینجاست که سیستم عامل ها معمولا در حافظه RAM سیستم یا در حافظه ی هارددیسک نگهداری می شوند، اما Firmware ها در حافظه ی ROM سیستم نگهداری می شوند و تقریبا فقط خواندنی هستند.
- دقت کنید که این شما نیستید که Firmware یک دستگاه را نصب می کنید، بلکه کمپانی تولید کننده تجهیزات کامپیوتری در بدو ایجاد کردن سخت افزار مورد نظر، Firmware آن را نیز بر رویش نصب می کند.
- باید بدانید که BIOS سیستم شما نیز در واقع یک نوع Firmware است، زیرا هم در حافظه دائمی یعنی ROM قرار دارد و هم امکان اعمال یک سری کنترلهای اولیه را بر روی سخت افزار به شما می دهد و از طرفی شما نمی توانید تغییر چندانی بر روی ساختار BIOS ایجاد کنید.
- البته تجهیزات دیگری در کامپیوتر هستند که برای خودشان Firmware دارند، Network Cards، Graphics card، کنترلرهای RAID، Hard Drive، Flash Memory، حافظه های SSD، Sound Cards، مودم های ADSL و Router ها، همه و همه دارای Firmware هستند.
- دستگاه های روتر خانگی ، سرورهای فیزیکی ، همگی دارای Firmware هستند و بعضا شرکت سازنده امکان بروز رسانی آنها را با بسته های جدیدی از Firmware می دهد. بدیهی است با بروز رسانی Firmware دستگاه امکانات جدیدتری به آن اضافه خواهد شد.

➢ Buffer :

- حافظه ی Buffer، یک حافظه است به عنوان رابط، که میان دو سخت افزار بکار می رود، تا اختلاف سرعت دو دستگاه را جبران کند.
- مثلاً در Printer، یک بافر وجود دارد. چون سرعت چاپگر نسبت به سرعت کامپیوتر، خیلی پایین تر است. بنابراین بین پردازشگر و چاپگر، بافری (چه به صورت سخت افزاری و چه به صورت نرم افزاری) قرار می گیرد تا پردازشگر اطلاعات را برای بافر فرستاده و چاپگر بالاخره بداند که کدام صفحات را باید پرینت بگیرد و سر صبر و حوصله آنها را چاپ نماید و پردازشگر هم پس از فرستادن اطلاعات می تواند به کارهای دیگری برسد.
- بطور مثال گاهی روی هارد دیسک ها یا پرینترها درج می شود : Cache ودر مقابلش حجمی در حدود چند مگابایت قرار می گیرد. در حقیقت این همان حافظه ی بافر است و نه Cache ای که در پردازشگر وجود دارد.

➢ Cache و Buffer :

- Cache برای افزایش سرعت بکار می رود، اما Buffer برای هماهنگی سرعت.
- Buffer همیشه در دستگاه های با سرعت کمتر طراحی می شود، تا بتواند دستوراتی که با سرعت بالا آمده اند را حفظ و بررسی کند.
- شباهت Cache و Buffer این است که هردو، حافظه های فرار هستند، یعنی با قطع برق، اطلاعاتشان از دست می رود.

➢ UEFI (Unified Extensible Firmware Interface) :

- UEFI همان کنسول گرافیکی است که جایگزین BIOS سیستم شده است و تقریبا همه ی سیستم های سخت افزاری جدید به جای BIOS از UEFI استفاده می کنند.
- UEFI نیز نوعی Firmware است.
- به نوعی می توانیم UEFI را به عنوان یک BIOS مدرن و پیشرفته با توانایی های بالا در نظربگیریم.
- با تنظیماتی که در BIOS وجود دارد می توانیم انتخاب کنیم که از قابلیت های UEFI استفاده بکنیم یا خیر.
- اصطلاح UEFI BIOS به UEFI اشاره دارد و Legacy BIOS به BIOS.
- می توان سیستم عامل را در حالت UEFI نصب کرد، که البته شرایطی هم دارد که در ادامه توضیح می دهیم.

➢ Hot swap and Hot plug :

▪ **Hot plugging** به فرآیند اضافه یا جایگزین کردن یک سخت افزار به یک سیستم روشن گفته می شود، طوری که نیازی به راه اندازی مجدد سیستم (restart کردن) نباشد.

سخت افزارهایی که درحین کار سیستم عامل می توانند به کامپیوتر متصل شده و بدونی نیاز به restart، قابل استفاده باشند و خللی در کار سیستم بوجود نیاورند، Hot plug device یا Hot-pluggable device نامیده می شوند.

مثل: Mouse , Keyboard , Flash memory و ... .

▪ **Hot swapping** به فرآیند اضافه یا جایگزین کردن یک سخت افزار به یک سیستم روشن گفته می شود، طوری که نیازی به «ابتدا خاموش کردن سیستم، و سپس اضافه یا جایگزین کردن» آن سخت افزار نباشد.

سخت افزارهایی که درحین کار سیستم عامل، و بدون نیاز به Shutdown سیستم، می توانند به کامپیوتر متصل شده و قابل استفاده باشند و خللی در کار سیستم بوجود نیاورند، Hot swap device یا Hot-swappable device نامیده می شوند.

مثل: انواع Storage ها و ... .

➢ SLOT :

Slot یا درگاه، به شیارهایی روی **Mainboard** گفته می‌شود که می‌توانیم در آنها قطعات جانبیِ کارت شکل قرار دهیم.

انواع **Slot** :

- **RAM Slot** : که فقط برای اتصال **RAM** به **Mainboard** است.
- **PCI Slot** : **PCI** مخفف **Peripheral Component Interconnect** به مفهوم اتصال سریع تجهیزات جانبی است.

این درگاه، برای کارتهای گوناگونی مثل **Modem**، **Network Card** ، **Sound Card** و ... استفاده می شود.

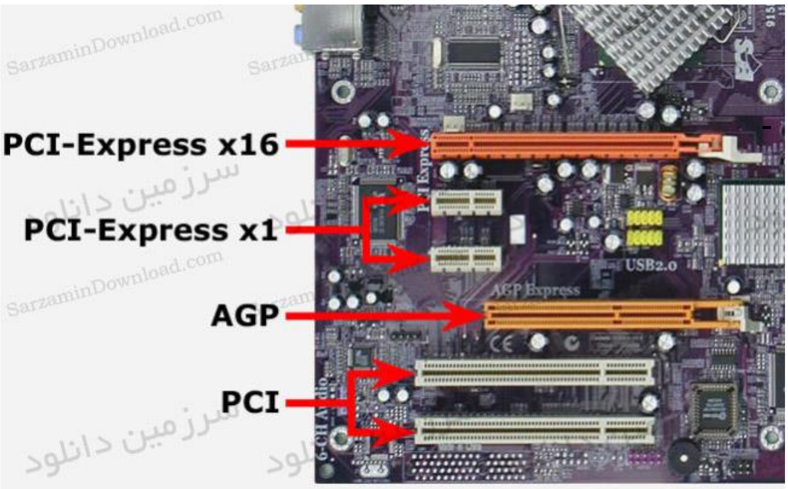
- **PCIe** : **e** مخفف **Express** می باشد. کاربرد آن مثل **PCI** است، اما سرعت انتقال داده در آن خیلی بیشتر است.
- **AGP** : اسلاتی قدیمی است که فقط برای اتصال کارت گرافیک استفاده می شد، اما امروزه کارت گرافیک را از طریق یکی از درگاه های **PCIe** متصل می کنند.

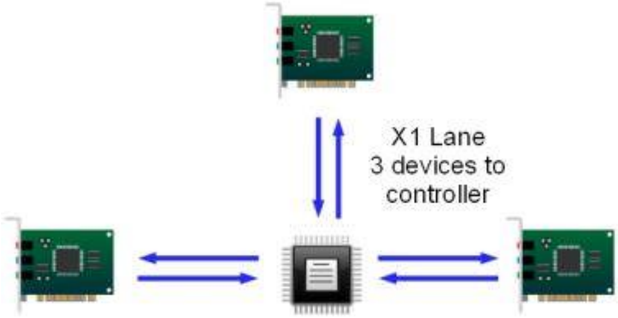
PCI :

- اساس کار **PCI** بر انتقال اطلاعات بصورت موازی است. یعنی به ازای هر بیت، یک سیم باید درنظر گرفته شود.
- مثلا برای یک انتقال **32** بیتی، **32** سیم روی **Mainboard** باید طراحی شود.
- در انتقال موازی، همه ی **32** بیت می توانند بطور همزمان عبور کنند.
- مشکلات درگاه **PCI** :
  - تأثیر میدان مغناطیسی تشکیل شده ی اطراف هر سیم، بر روی سیم های مجاور است؛ که آنرا اثر متقابل مسیرها بر یکدیگر گویند.
  - ایجاد تأخیر زمانی در ارسال و دریافت همه ی بیت ها
  - عدم قابلیت ارسال و دریافت همزمان داده ها، ابتدا باید سیگنال ارسالی برسد و دریافت شود، سپس سیگنالی می تواند بعنوان سیگنال بازگشت فرستاده شود؛ که به این ویژگی **Half Duplex** گفته می شود.

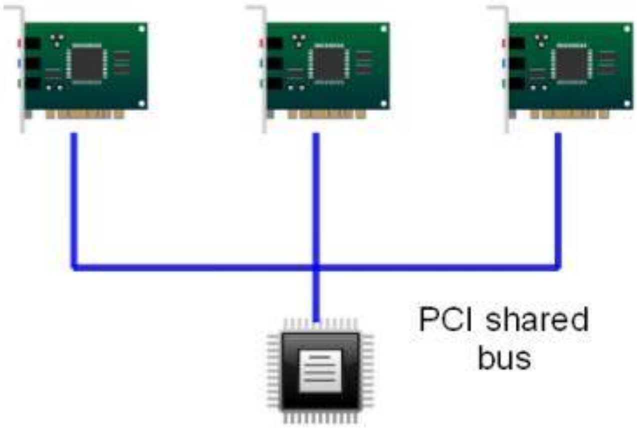
PCIe :

- اولین ورژن **PCIe** در سال **2003** و با سرعت انتقال داده ی **2.5** گیگا بر ثانیه معرفی شد.
- معمولاً **PCI Express** را در مورد کارت‌ها به کار می‌بریم و **PCIe** را برای اشاره به اسلات‌های مربوطه روی مادربورد استفاده می‌کنیم.
- در درگاه **PCIe** ، انتقال اطلاعات به صورت سری یا سریال انجام می شود، به این معنی که در هر لحظه فقط یک بیت ارسال می شود.
- یکی از مزایای **PCIe** این است که مقدار اثرمتقابل مسیرها بر یکدیگر در مادربردها، به خاطر مدارات نقطه به نقطه کاهش می یابد، چون از ۴ مسیر به جای ۳۲ مسیر برای هر ارتباط پایه استفاده شده است.
- اسلات‌ها و کانکتورهای **PCI Express** دارای تعداد زیادی پین می‌باشند که علاوه بر انتقال دادن داده، می‌توانند مقدار زیادی توان مصرفی را هم به کارت جانبی تحویل دهند. البته به این مورد باید توجه کنید که منظور از کانکتور، بخشی از کارت **PCI Express** می‌باشد که شامل پین‌های مسی است که در اسلات **Mainboard** وارد می‌شود.
- **PCIe** بر اساس مسیرهایی به نام **Lane** یا خط ارتباطی کار می کند، که هر **Lane** شامل **4** سیم است.
- هر **Lane** شامل دو مسیر ارسال و دریافت است. پس دو سیم را به مسیر ارسال و دو سیم را به مسیر دریافت اختصاص می دهد.
- پس در **PCIe** حداقل به **4** سیم نیاز است.
- هر **Lane** بصورت تک بیتی و ارسال و دریافت همزمان و دو طرفه کار می کند؛ که به این ویژگی **Full Duplex** گفته می شود.
- هرچه تعداد **Lane** ها بیشتر باشد، داده ی بیشتری عبور کرده و پهنای باند بیشتر خواهد شد.
- **Lane** ها را با حرف **X** و تعدادشان را با عددی در کنار آن نشان می دهند. مثلاً **X8** یعنی دارای **8 Lane** .
- معماری **PCIe** یک معماری **Point to Point** است، به این معنی که هر یک از وسایل می‌تواند با دیگر وسایل رابطه برقرار کند.





در PCI قدیمی، ارتباط موازی، راه را برای حالت نقطه به نقطه بسته بود و سه کارت اشاره شده، باید در ابتدا با هم هماهنگ شده و در نهایت به باس ارتباطی متصل می‌شدند. پهنای باند کمی که PCI داشت هم بین سه کارت به صورت مشترک استفاده می شد و این یعنی سرعت کمتر.



- کارت‌های طراحی شده برای کوچک‌ترین اسلات PCIe یعنی X1 در ابتدا کمتر از 10 وات انرژی مصرف می‌کردند، اما بعدها با طراحی بزرگ‌تر و تحت نام Full Height به توان مصرفی بیشتری در حد 25 وات نیاز پیدا کردند.

- در صورت بالا بودن ظرفیت اسلات PCI Express، از کابل برق 6 یا 8 پینی استفاده می‌شود. کابل 6 پینی می‌تواند حداکثر تا 75 وات و کابل 8 پینی می‌تواند حداکثر تا 150 وات توان الکتریکی را در اختیار کارت گرافیک قرار دهد.

- برای مثال اگر کارت گرافیک شما دو هسته‌ای باشد، دو کابل 8 پین و استفاده از اسلات PCI Express 3.0، می‌تواند 375 وات توان مصرفی را دریافت کند. البته در صورت بیکار ماندن، این مقدار توان بسیار کم می‌شود.

- PCIe از نظر سازگاری با نسخه های قدیمی مشکلی ندارد. و البته کارتی که دارای تعداد مسیر کمتری می‌باشد، در اسلات بزرگ‌تر هم قابل استفاده می‌باشد. برای مثال کارت x1 با اینکه پهنای اسلات PCIe x16 را نمی‌پوشاند، اما بدون هیچ مشکلی کار می‌کند. پس این نتیجه حاصل می‌شود که کافیست فقط کارت جانبی را روی اسلات Mainboard به درستی قرار دهیم.

- در صورت انتخاب کارت گرافیکی با مصرف کم، معمولاً در استفاده از آن روی پی‌سی‌آی اکسپرس مشکلی پیش نمی‌آید. اما در مقابل کارت گرافیکی پرمصرف همانند "PCI-Express 3.0" وجود دارد که در صورت استفاده روی مادربوردهای قدیمی و متعلق به سال 2010 و قبل‌تر، با مشکل مواجه خواهیم شد و احتمال اینکه درست کار نکند وجود دارد.

HDD (Hard Disk Drive):

بسته به کاربرد و استفاده از **Hard Disk** ها، شامل دو دسته هستند:

- **Enterprise-Class Disk** : جهت استفاده در سیستم های **Server** هستند که پایداری و قدرت بالایی دارند.
- **Consumer-class Disk** (Desktop-Class) : جهت استفاده در سیستم های معمولی یا **Client** هستند.

➢ Dimensions :

- **1.8** اینچی :
- **2.5** اینچی: ابعاد **HDD** های مورد استفاده در **Laptop** ها و نوت بوک ها، همیشه از نوع **2.5"** می باشد.
- **3.5** اینچی: که به آن **Full Size** یا **Desktop** نیز می گویند، در کامپیوترهای **Desktop** یا **Server** استفاده می شود.

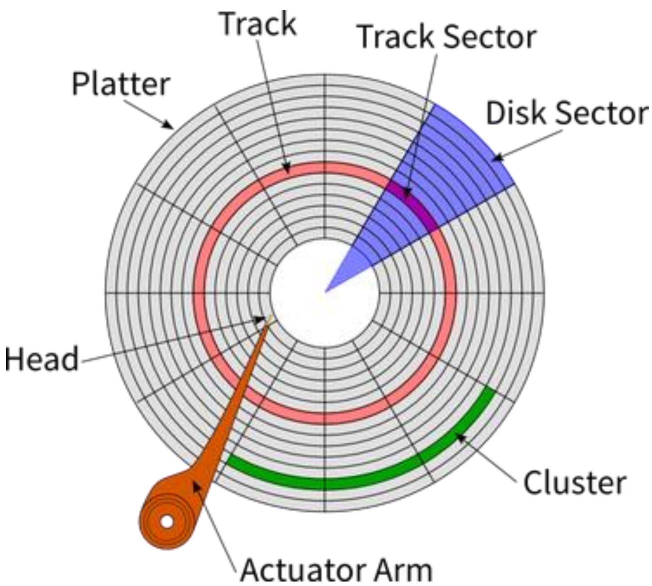
- هارد دیسک های **2.5** اینچی کند تر هستند، برق کمتری مصرف می کنند و مقاومت به ضربه و تکان در آنها بیشتر است.
- نوع **1/8** اینچی، در **mp3 player** ها و **Notebook** های کوچک مورد استفاده قرار می گیرد. مصرف انرژی بسیار کمی دارند و در مقابل ضربه، بسیار مقاوم هستند.



➢ RPM (Revolutions per minute) :

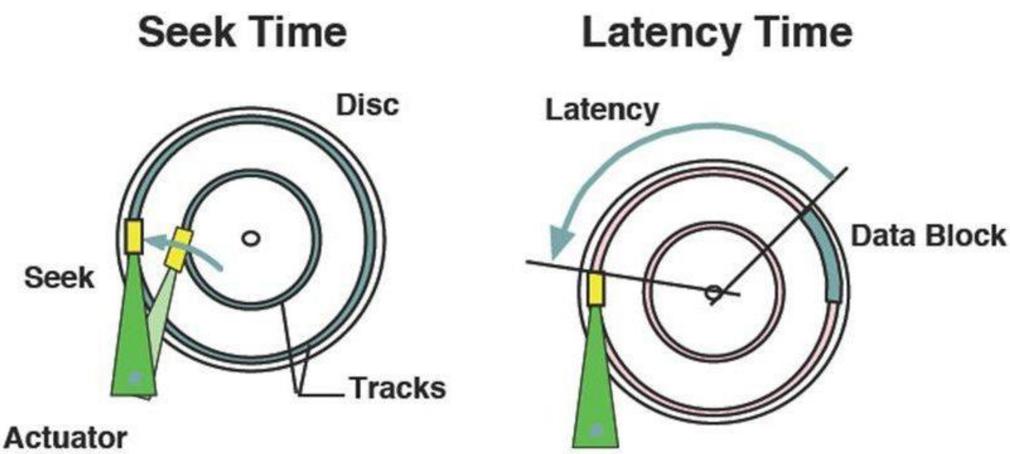
- **HDD** ها حداقل از یک دیسکِ گردان بنام **Platter** و یک جسم نوک تیز بنام **Head** تشکیل شده اند که **Platter** می چرخد و **Head** اطلاعات روی آن را می خواند.
- به همین دلیل، مشخصه ای بنام **RPM** یا «چرخش در دقیقه» وجود دارد که تعداد چرخش های **Platter** را نشان می دهد که هرچه این نرخ بیشتر باشد، سرعت هارد بالاتر است.
- یکی از مزایای دیسک‌های سخت نسبت به دیسک های **SSD**، این است که می‌توانند حجم زیادی از اطلاعات را در ازای قیمت ارزان برای شما نگهداری کنند.
- از معایت این چرخش ها و حرکات مکانیکی در **HDD**:
  - ❖ کاهش سرعت
  - ❖ اتلاف توان باتری در لپ تاپ ها

تاخیر متوسط [میلی‌ثانیه - ms]	سرعت چرخش صفحات (RPM)
2	15000
3	10000
4.16	7200
5.55	5400
6.25	4800



⮚ Seek Time :

- حرکت Head، در محدوده ی شعاع Platter هاست که در نتیجه فقط به جهت تغییر Track برای خواندن داده ها، حرکت می کند.
- وسیله ای که Head را بر روی Track ها جابجا می کند، بازوی متحرک یا Head Arm (Actuator arm) نام دارد.
- به مدت زمان لازم برای حرکت بازوی متحرک، تا رساندن Head به Track مورد نظر، Seek Time (زمان جستجو) می گویند.
- به آن Access Time هم گفته می شود، اما در واقع Access Time کمی طولانی تر از Seek Time است، چون دسترسی به داده، زمانبرتر از یافتن آن است!
- واحد Seek Time را معمولاً به میلی ثانیه (ms) بیان می کنند.
- هرقدر میزان Seek Time کمتر باشد، مدت زمان دسترسی به داده های روی هارد دیسک نیز کاهش یافته و سرعت Read در هارد دیسک افزایش می یابد.
- میزان Seek Time در سخت افزارهای مختلف:
  - HDD : 8 ms – 9 ms
  - Powerful Servers : 4 ms
  - Smart phone : 12 ms
- با توجه به اینکه در درایوهای نوری و Floppy Disk ها اندازه ی Head بزرگ است، میزان Seek Time تا 65 الی 75 میلی ثانیه هم خواهد بود، که سرعت و کارآیی پایین می آید.
- اگرچه راهی برای افزایش Seek Time وجود ندارد، اما می توان با عملیات Defragment کردن پارتیشن ها، آن را کاهش داد.



➢ latency time (Rotational latency):

زمان تاخیری که تاخیر چرخشی هم نامیده می شود، زمانی است که طول می‌کشد تا **Platter** بچرخد که **Sector** مقصد، در زیر **Head** قرار بگیرد.

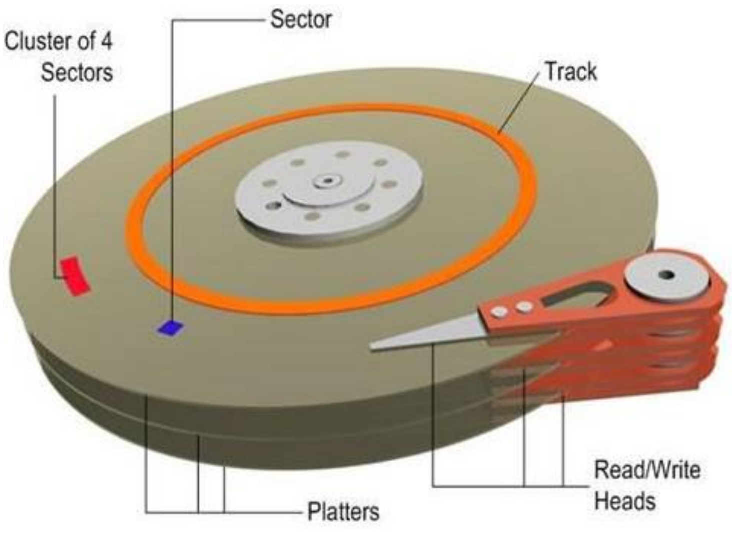
هرچه دیسک سریعتر بچرخد، زمان کمتری برای چرخش سکتور در زیر **Head** لازم است.
هر چه **Head** به بخش مورد نظر نزدیکتر باشد، زمان کمتری برای چرخش سکتور در زیر **Head** لازم است.

عوامل دیگری نیز وجود دارند که می توانند بر این زمان، تأثیر بگذارند، مثل تعداد **Platter** ها و ضخامت **Platter** ها و ... .

در جدول زیر میانگین **latency time** برای سرعت های مختلف چرخش **HDD** را می بینیم:

RPM	Latency Time (ms)
5400	5.56
7200	4.17
10000	3.00
15000	2.00

➢ HDD Structure :



- یک دیسک ذخیره سازی، شامل چند صفحه به نام **Platter** می باشد.
- کوچکترین بخش در هر **Platter**، یک **Sector** است.
- از مجموع چند **Sector** در کنار هم، یک **Cluster** تشکیل می شود.
- تمام **Sector** هایی که در یک ردیف قرار دارند، یک **Track** را تشکیل می دهند.

کوچکترین فضا یا ظرفیت در هر **Hard Disk**، برابر است با اندازه یا ظرفیت یک **Sector** در آن **Hard Disk**. به آن **Sector Size** می گویند.
یعنی کوچکترین محل نگه داری داده ها، در یک دستگاه **Hard Disk**، به اندازه ی یک **Sector** در آن می باشد.

- در **HD** های قدیمی، میزان **Sector Size** برابر بود با **512 Bytes**.
- در **HD** های جدیدتر، میزان **Sector Size** برابر است با **4096 Bytes** یا **4 KiloByte**.

فرض کنید بخواهیم یک فایل یک مگابایتی را در هردو حافظه های قدیمی و جدید ذخیره کنیم.
در عمل، در HD قدیمی، تعداد Sector هایی که به این فایل اختصاص داده می شوند، بیشتر از تعداد Sector هایی خواهند بود که در HD جدید به آن اختصاص داده می شوند.

در حقیقت میزان Sector Size را توسط پارامتری به نام AUS (Allocation Unit Size) تعریف می کنیم.

- هرقدر که میزان AUS را بزرگتر درنظر بگیریم، سرعت اجرای فایل های حجیم، بیشتر خواهد شد.
- درحالی که اگر بیشتر با فایل های کوچک و کم حجم کار می کنیم، باید میزان AUS را کمتر درنظر بگیریم.

- **اگر میزان AUS را بزرگ بگیریم و با فایل های خیلی کوچک کار کنیم، می بینیم که به سادگی ظرفیت حافظه، پر خواهد شد. چرا که هر فایل، با هر اندازه ای، درون هر تعداد Sector ای که قرار بگیرد، احتمالاً بخشی از آخرین Sector اش، خالی می ماند، که چون آن Sector هم به آن فایل اختصاص داده شده است، برای فایل های دیگر، قابل استفاده نخواهد بود.**

- **اگر میزان AUS را کوچک در نظر بگیریم و با فایلهای خیلی بزرگ کار کنیم، مقدار زمان پیدا کردنِ Sector ها (Seek Time) بیشتر می شود که باعث افزایش تأخیر در اجرای فایل ها می شود.**

یک استاندارد وجود دارد که طبق آن:

- **اگر ظرفیت دیسک کمتر از 16 ترا بایت باشد، AUS را برابر با 4096 بایت در نظر می گیریم.**
- **اگر ظرفیت دیسک بیش از 16 ترابایت باشد، AUS را برابر با 16 کیلو بایت در نظر می گیریم.**

از طرف دیگر، جدا از میزان ظرفیت HD، اگر دارای فایل های پیوسته و بزرگتر از 500 Mega Byte باشیم، مثل ویدیوها؛ باز هم AUS را 16 KB یا بیشتر، در نظر می گیریم.

➢ Interface :

- **همان بخشی از دستگاه حافظه است که با استفاده از کابل مخصوص Data، هارد را به Mainboard متصل می کند.**
- **Interface های رایج:**

- **SCSI : مخفف Small Computer Systems Interface است که اشاره دارد به کابل و سوکتی برای وصل شدن چاپگر و یا هر دستگاهی که اجازه ی اتصال به خروجی SCSI را دارد.**
  - **سرعت انتقال داده ها در سال ۱۹۸۶ به ۵ مگابایت بر ثانیه می رسید.(همان سالی که بطور رسمی تولید و منتشر شد.)**
  - **انتقال اطلاعات بصورت موازی (parallel) انجام می شود.**
  - **امروزه Hard های با این نوع درگاه، در هیچ motherboard ای پشتیبانی نمی شوند.**
- **PATA : مخفف Parallel Advanced Technology Attachment است که کابلی پهن و عریض بوده که بر پایه ی تکنولوژی قدیمی تر یعنی IDE است، اما سرعت بالاتری دارد.**
  - **به سبب یکسان بودن سوکتِ اتصال آن با IDE، آن را نیز با IDE می شناسند.**
  - **این کابل دارای تعداد زیادی Pin در روی سوکتش بود که مثلاً اگر دارای 40 پین بود، 20 پین همزمان عملیات ارسال داده و 20 پین عمل دریافت را انجام می دادند.**
  - **این نوع درگاه، قابلیت Hot Plugging را پشتیبانی نمی کند.**
- **SATA : مخفف Serial ATA می باشد که داده ها را بصورت سریال** (پشت سر هم) **ارسال می کند.**
  - **SATA دارای نسخه های SATA I ، SATA II و SATA III می باشد.**
  - **جدول زیر سرعت انتقال DATA را در نسخه های مختلف SATA نشان می دهد:**

SATA Version	Speed Rate
SATA I	1.5 Gb/s یا 150 MB/s
SATA II	3 Gb/s یا 300 MB/s
SATA III	6 Gb/s یا 600 MB/s

- با توجه به اینکه درگاه های Sata در Hard ها، می توانند دارای ورژن های متفاوت SATA باشند و از طرفی برای هر ورژن از SATA یک کابل مختص خودش وجود دارد.
- می توانیم هر نسخه از درگاه SATA روی HDD را (نسخه 1 یا 2 یا 3)، به هر نسخه از Sata-Interface روی Mainboard، توسط یکی از نسخه های کابل SATA (نسخه 1 یا 2 یا 3) متصل کنید و از هارد استفاده کنید!
- اما درنتیجه آن Interface ای که ورژن و سرعت پایین تری دارد (HDD یا Cable و یا Mainboard) تعیین کننده ی حداکثر سرعت انتقال اطلاعات خواهد بود!

SAS (Serial Attached SCSI):

- در مقایسه با SCSI های قدیمی، از کارایی های بسیار بالاتری برخوردار است.
- جدول زیر سرعت انتقال DATA را در نسخه های مختلف SAS نشان می دهد:

SAS Version	Speed Rate
SAS I	3 Gb/s
SAS II	6 Gb/s
SAS III	12 Gb/s
SAS IV	22.5 Gb/s

- می توان همزمان حداکثر 128 دستگاه جانبی مختلف با کابل های کوتاه و بلند را از طریق این درگاه متصل کرد.
- برخلاف SCSI های قدیمی، می توان توسط این تکنولوژی، دستگاه ها را بصورت Hot Plug استفاده کرد.
- برخلاف SCSI های قدیمی، انتقال اطلاعات، به صورت ترتیبی (Serial) و یا نقطه به نقطه (Point to Point) است.
- در حقیقت در تکنولوژی SATA نوع ارتباط Serial است، اما نوع درگاه Parallel است، در حالی که در SAS نوع ارتباط سریال است و نوع درگاه Serial Bus می باشد.
- سرعت اتصالات Serial Bus از اتصالات Parallel بالاتر است، چون پهنای باند مختص به خود را داشته و اشتراکی نمی باشد.
- دستگاه هایی که از SAS استفاده می کنند، از دستگاه هایی که از SATA و SCSI استفاده می کنند نیز پشتیبانی می کنند و می توانند با هم ارتباط برقرار کنند.
- اگر یکی از مسیرهای ارتباطی برای SAS قطع شود ، همچنان ارتباط می تواند از طریق مسیری مجزا و مستقل ادامه پیدا کند.
- می توان همزمان هم از قابلیت SAS و هم از قابلیت SATA استفاده کرد، در حالی که این قابلیت برای IDE و SCSI وجود نداشت!
- این هارد دیسک ها نیاز به دستگاه Power قدرتمندتری برای اجراء دارند، به همین خاطر در سرورها استفاده می شوند.

Buffer size :

- زمانی که کاربر، درخواست اطلاعاتی می کند، هارد دیسک علاوه بر اینکه فراخوانیِ داده را انجام می دهد، آنها را در فضایی کوچک در درون خودش، بطور موقت نیز ذخیره می کند، که این فضا را Buffer می گویند و دارای یک حجم معین می باشد.
- در صورتی که CPU، درخواست مجدد همان اطلاعات قبلی را داشته باشد، آنها را از طریق Buffer هارددیسک فرا می خواند.
- در موارد استفاده از برنامه های گرافیکی، ظرفیت هشت مگابایت یا بیشتر برای بافر، اثرات مثبتی را در رابطه با افزایش کارائی بدنبال خواهد داشت.

Model :

- هر هارد دیسک، یک شماره ی معرف دارد، که ترکیبی از حروف و اعداد است، و آن هارد را در میان تمام هاردهای دیگری که از شرکت تولید کننده اش وجود دارند، منحصربفرد می کند.

SSD (Solid-state drive) :

- SSD منبع ذخیره سازی ای است که از نیمه رسانایی جامد (Semiconductor) تشکیل شده است.
- از این تکنولوژی در ساخت حافظه های Flash نیز استفاده می شود.
- در اندازه های 1.5 و 2.5 و 3.5 اینچی تولید می شود.

- در SSD ها بر خلاف HDD ها، هیچ قسمت متحرکی وجود ندارد.
- HDD الکترومکانیکی است و SSD الکترونیکی.
- برای اتصال حافظه های SSD، حتی کابل های پرسرعت SATA 3 جوابگوی سرعت بالای آنها نبودند. پس Interface های دیگر پدید آمدند. که بطورکلی دو دسته اند:

- SSD **که از پهنای باند و مسیر** SATA **استفاده می کند (**SATA-SSD**):**
  - درگاه و پروتکل مورد استفاده در اغلب این نوع SSD ها، SATA III می باشد.
  - شامل دو دسته می شود:

❖ **Standard SATA-SDD** : که درست مثل یک درایو HDD باید توسط کابل Data و Power به Mainboard متصل شود.

❖ **mSATA-SSD (miniSATA)**: از نوعی درگاه اتصال به نام mSata استفاده می کند که تکنولوژی ارسال و دریافت در آن، SATA است، (از SATA-Bus استفاده می کند.) به همین جهت شکل ظاهری این SSD ، نوعی کارت است که باید در Slot گیره مانند mSata که روی Mainboard قرار دارد، جای گرفته و در طرف دیگر پیچ شود. از لحاظ ظاهری کارتی کوچک است که دارای یک شیار می باشد.

❖ **SATA-M.2-SSD :**

- Interface آن M.2 است.
- M.2 نوعی Slot است که از لحاظ ظاهری، شبیه به mSATA است اما از لحاظ نوع تراشه ی ورودی، متفاوت است.
- از پهنای باند و مسیر SATA برای ارسال و دریافت ها استفاده می کند (SATA-Bus).
- شکل ظاهری این SSD هم مثل mSATA-SSD ، نوعی کارت است که باید در Slot گیره مانند M.2 که روی Mainboard قرار دارد، جای گرفته و در طرف دیگر پیچ شود.
- از لحاظ سرعت، تفاوت چندانی با mSATA-SSD ندارد، چون هردو از SATA-Bus بهره می برند.
- از لحاظ نوع سوکت M.2، دو نوع هستند:
  - ➢ X2 : از دو مسیر ارتباطی که دارای نوعی Key ID است بنام B استفاده می کند.
    (Key ID به دلیل تعیین مکان قرارگیری شیار تراشه است.)

که باید دقت کرد که هم تراشه ی ورودی هارد و هم اسلات M.2 روی مادربورد از نوع B باشند. اگر نباشند هم، مشکل خاصی پیش نمی آید.

  - ➢ X4 : از چهار مسیر ارتباطی که دارای نوعی Key ID است بنام M، استفاده می کند.
    باید دقت کرد که هم تراشه ی ورودی SSD و هم اسلات M.2 روی مادربورد از نوع M باشند، اگر نباشند، از هر چهار مسیر ارتباطی هارد استفاده نخواهد شد و به حداکثر سرعت ممکن نخواهید رسید.

- SSD **که از پهنای باند و مسیر** PCIe **استفاده می کند** (PCIe-SSD)**:**
  - از پهنای باند و مسیر **PCIe** برای ارسال و دریافت ها استفاده می کند (از **PCI-Bus** استفاده می کند).
  - سرعتی چهار برابر بالاتر از **mSata-SSD** دارد.
  - به دلیل نیاز به درگاه **PCIe**، فقط در سیستم های **desktop** استفاده می شود.
  - مناسب سیستم های صنعتی است.
  - **PCIe-SSD** ها از لحاظ پروتکل ارتباطی، دو دسته دارند:
    - از کنترلر **AHCI** یا **Advanced Host Controller Interface** برای ارسال و دریافت اطلاعات استفاده می کنند، که اصلاحاً این گونه هاردها را **AHCI-SSD** نیز می گویند.
    - از کنترلر **NVMe** یا **Non-Volatile Memory Express** برای ارسال و دریافت اطلاعات استفاده می کنند که اصلاحاً این گونه هاردها را **NVMe-SSD** نیز می گویند؛ و سرعت بالاتری از **AHCI-SSD** ها دارند.

  - **PCIe-SSD** ها از لحاظ درگاه نصب سخت افزاری دو نوع هستند:
    - **Standard PCIe-SDD** : که درست مثل یک کارت با سوکت **PCIe**، در درگاه **PCIe** مادربرد قرار می گیرد.
    - **M.2 PCIe-SDD** : از **M.2 Interface** استفاده می کند. که از لحاظ ویژگی های نصب سخت افزاری، مشابه با **M.2 SATA SSD** می باشد، اما نوع ارتباطش، **PCIe** است.

- هنگام خرید **M.2-SSD** باید توجه کنید که سوکت **M.2** موجود روی **Mainboard** شما چیست، و **SSD** ای را خریداری کنید که مطابق سوکت **M.2** مادربرد شما باشد. چرا که نمی توان یک **PCIe-M.2-SSD** را روی سوکت **M.2** ای نصب کرد که از **SATA-Bus** استفاده می کند و یا یک **SATA-M.2-SSD** را روی سوکت **M.2** ای نصب کرد که از **PCIe-Bus** استفاده می کند.

- می توان **M.2 PCIe x2 SSD** را روی سوکت **M.2 PCIe x4** نصب کرد، البته **2** مسیر از سوکت **M.2** بدون استفاده خواهند ماند؛ و برعکس می توان **SSD PCIe x4** را روی سوکت **M.2 PCIe x2** نصب کرد، اما نمی توان از حداکثر سرعت **SSD** بهره برد، زیرا در این حالت، **SSD** به **4** مسیر **PCIe** نیاز دارد، در حالی که **Mainboard** تنها **2** مسیر در اختیارش قرار می دهد.

- استفاده از هاردهای **SSD** مزایای زیر را بدنبال خواهد داشت:
  - توان مصرفی کم : کاهش مصرف برق و به تبعیت از آن کاهش مصرف باتری لپ تاپ؛
  - بالا بودن سرعت خواندن/نوشتن اطلاعات، به این جهت که قطعات متحرک مثل **Head** ندارند، پس **Seek Time** هم عملاً در این دیسک ها بی معنی است. اما اگر بخواهیم **Seek Time** دیسک های **SSD** را بیان کنیم؛ چیزی در حدود **0.08** و یا **0.16** میلی ثانیه **Seek Time** دارند.
  - بالا بودن مقاومت هاردهای **SSD** در مقابل ضربه؛
  - بی سر و صدا بودن و تولید گرمای بسیار کمتر؛
  - میدانهای مغناطیسی قوی می توانند به اطلاعات **HDD** آسیب برسانند اما **SSD** در برابر میدان مغناطیسی آسیب نمی بینند.

- یکی از نقاط ضعف **SSD** عدم امکان بازیابی داده هاست.

زمانیکه **HDD** از کار می افتد کارشناسان اغلب قادرند حداقل مقداری از داده ها را بازیابی کنند . که این امکان در **SSD** ها وجود ندارد.

- یک **Firmware** در حافظه ی درایوهای **SSD** قرار دارد و توسط مغز آن (کنترلر) اجرا و پردازش می‌شود.
- **Firmware** درایوهای **SSD** مدام تحت توسعه و بهبود هستند و از سوی سازنده، **Update** هایی برای آن‌ها منتشر می‌شود. پس بهتر است که همواره **Firmware** درایوهای **SSD** را برای در دسترس بودن نسخه ی جدیدتر بررسی کرد.

- **سیستم حذف فایل ها در SSD کمی پیچیده است، طوری که ابتدا باید صبر کرد تا فایل های انتخاب شده برای حذف، به یک حد نصاب برسند تا خود هارد SSD آنها را با هم و یک جا حذف کند، و در نتیجه تا زمانی که این فایل ها به حد نصاب نرسیده اند، فقط از نظر کاربر حذف شده اند، اما هنوز هستند و در صف تیک خورده ها برای حذف قرار گرفته اند و این قضیه، بعد از مدتی، سرعت این هاردها را کاهش می دهد.**
- **در نتیجه تکنیکی به نام Trim پدید آمد که با فعال کردن آن، دیگر نیازی به پر شدن سطل زباله ی این هارد و رسیدن فایل های دورریخته شده به حد نصاب و سپس حذفشان نیست، بلکه بطور اتوماتیک هر فایل در هر لحظه که تیک حذف شدن می خورد، کاملاً حذف خواهد شد. اما پیش نیاز این تکنیک این است که هم سیستم عامل و هم هارد SSD این قابلیت را پشتیبانی کنند یا به قولی Trim Support باشند و سپس این تکنیک را در سیستم عامل بصورت دستی فعال کرد.**
- **همان گونه که گفتیم SSD ها هیچ اجزای متحرکی درونشان ندارند، پس Fragmentation و Defragmentation در این گونه ذخیره ساز ها بی معنی است. چون نه تنها این کار یک اتلاف وقت به شمار می آید، بلکه از طول عمر دیسک SSD هم می کاهد.**

نکته: SSD Hard را هیچگاه Defrag نمی کنیم، چون باعث خرابی یا کاهش عمر مفید آن خواهد شد.

SSHD :

نوعی از هارددیسک ها وجود دارند که SSHD نامیده می شوند، و ترکیبی از هاردهای HDD و SSD هستند.
در حقیقت کاربر، دسترسی و کنترلی به بخش SSD ندارد! چون این Storage ها فقط برای بخش Cache خود، بطور کامل از یک هارد SSD داخلی استفاده می کنند.
سرعت این هاردها از هاردهای HDD بیشتر و از هاردهای SSD کمتر است.

: Common properties of Storages

:Naming the Disks

- در نرم افزارها یا در سیستم عامل های بر پایه ی لینوکس، هر دستگاه ذخیره سازی دارای یک نام خاص است.
- فرمتِ نام دستگاهی که Interface آن SATA باشد، به صورت مقابل می باشد: **SDX**
- **SD** مخفف **SATA Disk** می باشد.
- **X** مقداری بین **A** تا **Z** می باشد، که برای هر دستگاه، متفاوت خواهد بود.

مثلاً وقتی سه دستگاه **Storage** داشته باشیم، نام آنها، به صورت **sda** ، **sdb** ، **sdc** می باشد.

: File System

File System ابزاری نرم افزاری ست برای مدیریت، سازماندهی، نگهداری و دسترسی به دادهای **Storage**.

- **File System** ، داده ها را به بهترین نحو ممکن، با ویژگیهای خاص سخت افزارمان تطبیق می دهد.

چرا وجود یک **File System** ضروری است؟

جدول زیر را که شامل سه فایل با نام و محتوای زیر است، در نظر بگیرید:

محتوای فایل	نام فایل
VsyB2GI	**Text1**
7s2UIlu	**Text2**
ay53e8yH	**Text3**

بدون **File System**، داده‌ها فقط بر روی حافظه ذخیره می‌شوند.

فرض کنید سه فایل بالا را در حافظه ی بدون **FS** ذخیره می‌کنیم. بنابراین ابتدا و انتهای فایل‌ها مشخص نمی‌شوند:

V [1]	s [2]	y [3]	B [4]	2 [5]	G [6]	I [7]	7 [8]
s [9]	2 [10]	U [11]	l [12]	l [13]	u [14]	a [15]	y [16]
5 [17]	3 [18]	e [19]	8 [20]	y [21]	H [22]	[23]	[24]

همانطور که می‌بینید داده‌های ما به خوبی بر روی حافظه ذخیره شده اند.

اما مثلاً اگر بخواهیم فایل **Text2** را بازیابی کنیم، درحالی که نه از محل قرارگیری اولین داده ی این فایل (عدد ۷، در مکان ۸) و آخرین آن (حرف **u** ، در مکان ۱۴) یا طول داده‌ها (۷ کاراکتر) اطلاعی نداریم، غیر ممکن است که بتوانیم فایل مورد نظر را به درستی بازیابی کنیم.

ذخیره و بازیابی توسط فایل سیستم :

V [1]	s [2]	y [3]	B [4]	2 [5]	G [6]	I [7]	7 [8]
s [9]	2 [10]	U [11]	l [12]	l [13]	u [14]	a [15]	y [16]
5 [17]	3 [18]	e [19]	8 [20]	y [21]	H [22]	[23]	[24]

همانطور که می‌بینید داده‌های ما به خوبی بر روی حافظه ذخیره شده اند و با توجه به مشخص بودم محل ابتدا و انتهای داده ها، فایل‌ها به صورت کامل و صحیح در دسترس خواهند بود.

- انواع File System ها در ویندوز عبارتند از :
  - Universal Disk Format (UDF) : امکان خواندن و نوشتن بر روی CD و DVD را فراهم می کند.
  - File Allocation Table (FAT) :
    - اکثر درایو های فلش یا کارت های حافظه از این فرمت استفاده می کنند تا علاوه بر رایانه ها، دستگاه های الکترونیکی دیگر نیز آنها را پشتیبانی کنند.
    - دارای ورژن های 12 ، 16 و 32 می باشد.
    - حجم فایل ها در FAT Partition ها نمی توانند بیشتر از 4 گیگابایت باشند.
    - حجم FAT Partition ها نمی توانند بیشتر از 8 ترابایت باشند.
    - سیستم عامل ها را نمی توان بر روی پارتیشن های FAT نصب کرد.
  - New Technology File System (NTFS) :
    - یکی از خصوصیات مهم آن، قابلیت recovery کردن است.
    - در هنگام نصب سیستم‌عامل ویندوز، فرمت System Drive شما را NTFS قرار خواهد داد.
    - برخی دستگاه های الکترونیکی، مثل کنسول های بازی، این FS را پشتیبانی نمی کنند.
    - NTFS یک یادداشت متنی از تمام فعالیتها را نگهداری می کند. می تواند پس از اینکه یک سخت افزار ذخیره سازی، بر اثر قطع برق یا هر اشکال دیگر خراب شد، دیسک را به حالت اولیه برگرداند، در حالیکه حافظه های FAT داده ها را از دست می دهند.
    - برخی از ورژن های Linux تنها توانایی خواندن اطلاعات از روی NTFS را دارند.
    - مزیت های NTFS که FAT فاقد آنهاست:
      - Compression
      - Encryption
      - Determination of Access level (تعیین سطح دسترسی)
  - Extended File Allocation Table (exFAT) :
    - به آن FAT 64 نیز می گویند.
    - از نسخه های قبلی FAT خیلی پیشرفته تر است.
    - سازگاری آن بیشتر از NTFS است.
  - Extended Filesystem (EXT) : این یک File System رایج در سیستم عامل Linux است که نسخه‌های مختلفی دارد.
  - Resilient File System (ReFS):
    - این FS به جهت رفع برخی از محدودیت های NTFS طراحی شد.
    - یکی از کمبودهای آن، این است که قابلیت Bootable شدن را ندارد.
    - جهت کنترل سیستم، در هنگام قطع جریان برق، بهتر عمل می کند.
    - ReFS فضاهای ذخیره سازی را بهتر شناسایی و مشکلات را بهتر رفع می کند.
    - برای Virtualization خیلی بهینه سازی شده است.

:Comparison of NTFS and ReFS ➢

Feature	ReFS	NTFS
Max file name length	255 Unicode characters	255 Unicode characters
Max path length	32K Unicode characters	32K Unicode characters
Max file size	35 PB (petabytes)	256 TB
Max volume size	35 PB	256 TB

Feature	ReFS	NTFS
BitLocker encryption	YES	YES
Data Deduplication	YES	YES
Cluster Shared Volume (CSV) support	YES	YES
Soft links	YES	YES
Failover cluster support	YES	YES
Access-control lists	YES	YES
USN journal	YES	YES
Changes notifications	YES	YES
Junction points	YES	YES
Mount points	YES	YES
Reparse points	YES	YES
Volume snapshots	YES	YES
File IDs	YES	YES
Oplocks	YES	YES
Sparse files	YES	YES
Named streams	YES	YES
Thin Provisioning	YES	YES
Offloaded Data Transfer (ODX)	NO	YES
Trim/Unmap	YES	YES

Feature	ReFS	NTFS
Block clone	YES	NO
Sparse VDL	YES	NO
Mirror-accelerated parity	Yes (on Storage Spaces Direct)	NO

Feature	ReFS	NTFS
File system compression	NO	YES
File system encryption	NO	YES
Transactions	NO	YES
Hard links	NO	YES
Object IDs	NO	YES
Short names	NO	YES
Extended attributes	NO	YES
Disk quotas	NO	YES
Bootable	NO	YES
Page file support	NO	YES
Supported on removable media	NO	YES

:Difference between quick format and format

هردوی این Format کردن ها، را با نام کلی Standard Format می شناسیم، که پس از انجام هردوی آنها، داده های گذشته، همچنان توسط نرم افزارهای قدرتمند، قابل بازیابی (Recovery) خواهند بود.

- **:Quick Format**

در این حالت بعد از فرمت کردن، درایو شما ممکن است خالی نمایش داده شود، اما در اصل فایل های گذشته، همچنان با یک نرم افزار recovery، به سادگی قابل باز گردانی خواهند بود.
در این روش، اگر ویروسی در flash یا Hard موجود بوده باشد، هنوز به صورت کامل پاک نشده است.

- **:Full Format**

در این مدل، یک مرحله به بهبود flash یا External Hard کمک می شود و به صورت خودکار، Sector های خراب، تعمیر می شوند. به همین دلیل، این فرمت، زمان بیشتری طول می کشد.
در این روش باز هم فایل ها قابل بازگردانی می باشند، اما از روش Quick سخت تر خواهد بود.

Disk Configuration :

بطورکلی دیسک ها را می‌توان به یکی از دو حالت Basic یا Dynamic پیکربندی کرد.

Basic :

- حالت Basic به سبب مدیریت آسان، محبوبیت بیشتری دارد.
- در این مدل، به هر منطقه ی مستقل حافظه، یک Partition گفته می شود.
- وقتی که یک Hard Disk دارای چند Partition در یک کامپیوتر روشن است، مثل این است که چند Storage به آن سیستم متصل هستند.
- هر Storage باید حداقل یک Partition داشته باشد.
- داده های هر Partition، نه می توانند با پارتیشن های دیگر share شوند و نه می توانند split (قطع) شده و در پارتیشن های دیگر ادامه یابند.
- برای تغییر و تعیین AUS یک Partition، روی آن کلیک راست کرده و Format و ... .

Dynamic :

- در دیسک هایی که به شیوه ی Dynamic مدیریت می شوند، به درایوهای حافظه، Volume گفته می شود، نه Partition.
- شیوه ی مدیریت Dynamic، بطور معمول در Server ها و سیستم هایی که نیاز به چندین سخت افزار ذخیره سازی دارند، استفاده می شود، مثل File Server ها.
- شیوه ی Dynamic، در رسانه های ذخیره سازی Portable کارآیی ندارد!
- Dynamic دارای چند نوع یا حالت است.
- مزایای دیسک های Dynamic :
  - نرخ Fault Tolerance بالا: تحمل پذیری در برابر ایجاد خطا یا مشکل یا قطع برنامه ها به علت نقص سخت افزاری و بازیابی مجدد اطلاعات در صورت از دست رفتنشان، بدون اخلال در سیستم و در دسترس ماندن.
  - توانایی بالا در رفع اشکالات
  - هر دیسک Dynamic دارای یک بانک داده برای ردیابی اطلاعات است؛ و هر دیسک، اطلاعات بانک خود را در دیسک دیگر، کپی می کند.
  - یکی از مشکلات مدیریت به شیوه ی Dynamic، این است که نمی توان بیش از یک سیستم عامل روی آنها نصب کرد.
  - از قابلیت مدیریت متمرکز داده‌ها برخوردار است. یعنی داده‌ها می‌توانند بروی چند دیسک پخش شده و مدیریت شوند.
  - دیسک Dynamic یک‌سری ویژگی‌های بیشتر و بهتر ارائه می‌دهد، که دیسک‌های Basic از انجام آن‌ها عاجزند:
    - می توان فضای یک Volume را بدون محدودیت گسترش داد؛ به این معنی که می توان یک درایو را بین چندین دیسک، پخش کرد.
    - می توان تعداد زیادی Volume داشت(نزدیک به 2000) که کارکردی شبیه به Primary Disk در Basic دارند.
    - ساده ترین نوع راه اندازی Volume برای یک دیسک Dynamic، به روش Simple Volume می باشد. متداولترین روش است که شبیه به Primary Partition است و در صورت استفاده از یک هارددیسک، فقط می توان simple volume داشت.

- برای تبدیل یک دیسک Dynamic به Basic ، باید از تمام داده ها Back up تهیه کرد، همه ی پارتیشن ها را خالی و حذف کرد، و سپس خواهیم توانست تبدیل را انجام دهیم. اما برای تبدیل یک دیسک Basic به Dynamic، نیازی به حذف داده ها نیست.

➢ Partition Table :

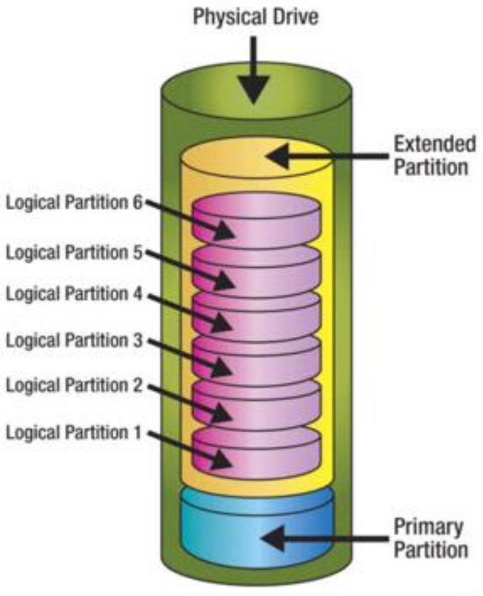
- برای مدیریت و کنترل Partition ها، از Partition Table یا جدول پارتیشن بندی، استفاده می شود.
- البته این Partition Table ها، برای مدیریت Volume های Dynamic هم استفاده می شوند.
- دو نوع Partition Table وجود دارد:

MBR (Master Boot Record):

Primary : یک پارتیشن استاندارد، از نوع **Primary** می باشد.

- ▪ می توان حداکثر چهار **Primary Partition** داشت.
- ▪ این مدل، فقط **Storage** های تا حجم دو **Terabyte** را پشتیبانی می کند.

نوع دیگری پارتیشن وجود دارد که برای رفع محدودیت های نرم افزاری این مدل پدید آمد، به نام **Extended**.
در حقیقت پارتیشن **Extended**، فقط نوعی قالب است، که قادر است فضایی که به آن اختصاص داده شده است را در زیر پارتیشن هایی کاملاً مشابه به پارتیشن **Primary** (به شکل نرم افزاری) تقسیم بندی کند.



- هریک از زیر پارتیشن هایی که در پارتیشن **Extended** ایجاد می شوند، **Logical Partition** نامیده می شوند.
- پارتیشن **Primary**، مستقل بوده و سرعت بیشتری دارد، اما **Logical** وابسته به فضای **Extended Partition** است.
- پارتیشن **Logical**، قابلیت **bootable** شدن ندارند، پس اگر ویندوز روی آن نصب شود، قابلیت اجرا شدن نخواهد داشت!
- پارتیشن **Primary** به طور مستقل و بطور سخت افزاری آدرس دهی می شود.
- پارتیشن های **Logical** فقط بطور نرم افزاری آدرس دهی می شوند.
- نامگذاری سخت افزاری پارتیشن های **Primary**، بصورت **SDX1** تا **SDX4** است.
- نامگذاری پارتیشن های **Logical**، بصورت **SDX5** تا **SDX16** می باشد.
- فقط یک **Extended Partition** می توان داشت،که جای یکی از پارتیشن های **Primary** را می گیرد.
- پس می توان یک پارتیشن **Extended** و سه پارتیشن **Primary** ساخت.
- در هنگام کار کردن در محیط سیستم عامل، هیچ تفاوتی میان پارتیشن های **Logical** و **Primary** مشخص نیست.
- حداکثراندازه ای که یک پارتیشن **Logical** می تواند دریافت کند، برابر است با اندازه ی تمام فضای پارتیشن **Extended**.
- حداکثر تعداد **Logical Partition** هایی که می توانیم داشته باشیم، دوازده عدد است.
- حداکثر حجمی که یک درایو **MBR** می تواند داشته باشد، حدود 2.2 TB می باشد.

- برای عملیات **Boot** شدن سیستم عامل توسط سیستم، یک **Sector** از پارتیشن **Primary** ای که سیستم عامل بر روی آن قرار دارد، به عنوان **Boot Sector** در نظر گرفته می شود که همچنین اطلاعات **Partition Table** نیز درون آن ذخیره می شوند.
- برای نصب ویندوز بر روی دیسک های **MBR** تنها می توان از **Bios Firmware** استفاده کرد و نه **UEFI**.

GPT (GUID Partition Table):

- در این نوع Partition Table، فقط می توان پارتیشن Primary داشت، و نه Extended امکانپذیر است و نه Logical.
- سیستم های 32 بیتی، این نوع Partition Table را پشتیبانی نمی کنند.
- Mainboard های قدیمی از GPT Style پشتیبانی نمی کنند.
- این Partition Table دستگاه های ذخیره سازی تا حجم یک Zettabyte را پشتیبانی می کند.
- حداکثر 128 پارتیشن Primary می توان ساخت.
- هر Partition می تواند تا 18 TB حجم داشته باشد.
- برای نامگذاری پارتیشن ها در محیط سیستم عامل، حروف A و B رزرو شده اند، پس از حرف C تا Z و یا ترکیب کلیه ی حروف الفبا می توان استفاده کرد.
- اطلاعات Partition Table، درون هریک از Partition هایی که ایجاد می کنیم، ذخیره می شوند.

- GPT دو یا سه Partition ضروریِ مخفی دارد: EFI-System Partition و OEM-Partition.
- برای اینکه یک GPT Disk بتواند Bootable باشد، از پارتیشن EFI-System استفاده می کند که اطلاعات Boot شدن را در خود داشته و بین 100 تا 260 مگابایت حجم دارد.
- برای نصب ویندوز توسط UEFI Firmware، باید دیسک در حالت GPT تنظیم شده باشد.
- اگر بخواهیم ویندوز را بر حافظه ای از نوع GPT نصب کنیم، هنگام کپی کردن ویندوز روی USB توسط نرم افزارهای مربوطه، باید Target System Type را بر روی GPT تنظیم کنیم.
- برای تبدیل مدل های GPT و MBR به یکدیگر، باید تمام داده های موجود در حافظه، در جایی دیگر ذخیره شوند، چرا که همگی حذف خواهند شد.
- برای تبدیل از مدل GPT به MBR، نباید حجم دستگاه Storage، بیشتر از 2 Terabyte باشد

Conversion GPT and MBR :

برای اطلاع از نوع Partition Table مربوط به یک Storage، دو روش وجود دارد:

➢ Disk Management :

وارد کنسول آن شده و در کادر پایین، سمت چپ، وارد Properties هریک از Disk ها شده و در تب Volumes.

➢ Diskpart :

در cmd درج می کنیم: diskpart و سپس list disk . در نتیجه هریک از دیسک ها که GPT باشد، دارای یک * است.

تبدیل این دو مدل به یکدیگر را هم می توان در همان کنسول Disk Management انجام داد و هم توسط دستورات Diskpart.

نکته: گاهی لازم است که قبل از آغاز نصب ویندوز، نوع Partition Table را تبدیل کنیم.

پس برای ورود به محیط cmd، باید قبل از ورود به ویزارد نصب ویندوز، دکمه های Shift+F10 را بفشاریم.

- وارد محیط Diskpart می شویم:

diskpart

- برای اطلاع از Disk Number درج می کنیم:

List disk

- دیسک موردنظر را انتخاب می کنیم:

Select disk <disk number>

- Partition Table را همراه با محتویات Storage کاملاً حذف می کنیم:

Clean

- دیسک را تبدیل می کنیم:

Convert MBR / GPT

CPU (Central Processing Unit):

CPU ها قطعاتی الکترونیکی از جنس Silicone هستند، که یک روکش سرامیکی با ابعاد بزرگتر، روی آنها را پوشانده است.

سیلیکون:

- یک عنصر طبیعی و نیمه رسانا است.
- بعد از اکسیژن، فراوان ترین عنصر در پوسته ی زمین است.
- در مقابل شرایط جوی مثل رطوبت، حرارت و نور، مقاومت بالایی دارد.
- تا دمای ۲۶۰ تا ۳۱۵ درجه سانتیگراد، خاصیت لاستیکی خود را حفظ می کند.
- تقریباً در همه ی صنایع، مخصوصاً درترکیب رنگها، صنعت لاستیک و روغنهای صنعتی بطور گسترده استفاده می شود.

دو شرکت بزرگ سازنده ی CPU:

- **Intel : که دارای دو نسخه است:**
  - **Core : برای کامپیوترهای خانگی و یا Client های با عملکرد سبک، به کار می رود.**

    خود به دو دسته تقسیم می شوند:
    - **Desktop : دارای مشخصه هایی با حروف اختصاری زیر هستند:**

      S : کم مصرف

      T : خیلی کم مصرف

      X : سرعت پردازش بیشتر
    - **Laptop : دارای مشخصه هایی با حروف اختصاری زیر هستند:**

      M (Mobile) **: سیار**

      Q (Quad)**: چهارهسته ای**

      H (High Processing) **: پردازش بالا**

      L (Low Power)**: کم مصرف**

      U (Ultra Low Power)**: خیلی کم مصرف**

      K (unlocked)**: جهت عملیات Over Clock**

    - **برای اطلاعات بیشتر در مرورگر می توانیم عبارت intel processors number را جستجو کنیم.**
    - **CPU های Core، دارای سه مشخصه ی عملیاتی نیز هستند:**
      - ✓ **Cores :**

        هر هسته در هر زمان، تنها یک دستور را می تواند اجرا و عملی کند.
      - ✓ **Threads :**

        قابلیتی ست که طی آن به صورت مجازی، تعداد هسته های موجود را بیشتر می کند، در نتیجه تعداد دستورهایی که در هر زمان، اجرا و عملی می شوند نیز بیشتر خواهد شد.
      - ✓ **Cache :**

        اطلاعاتی که مدام نیاز به دسترسی به آنهاست، توسط خود CPU به این حافظه ی درون CPU منتقل می شوند.

  - **Xeon : برای سیستم های Server یا سیستم های خیلی حرفه ای به کار می رود.**

برای شناسایی مدل و مشخصات یک CPU براساس مشخصات درج شده و موجود آن، مثال:

Processore Intel Core i7-5950 HQ

مدل: i7

نسل : 5

Processore Intel Core i7 970

مدل: i7

نسل: 1

- **AMD :**

قدرتمندترین و تنها نوع پردازشگر موجود از شرکت AMD، مدل Ryzen می باشد که شامل نسخه های زیر می باشد:

- **Ryzen 3** : سری 1000
- **Ryzen 5** : سری 2000
- **Ryzen 7** : سری 3000
- **Ryzen 9** : سری 3900 / سری 3950
- **Thread ripper**

نکات:

✓ پردازشگرهای AMD از خنک کننده های با کیفیت بالا برخوردار هستند.

✓ وقتی یک CPU Fan را تازه خریداری می کنیم، بر روی خودش خمیر سیلیکون وجود دارد و نیازی به اضافه کاری نیست.

✓ بهتر است که قبل از نصب مادربورد، CPU و Fan آن را نصب و سوار کنیم.

✓ CPU های Intel ای که قابلیت مجازی سازی را برای سیستم عامل، پشتیبانی و فراهم می کنند، دارای پسوند **VT-x** هستند.

✓ CPU های AMD ای که قابلیت مجازی سازی را برای سیستم عامل، پشتیبانی و فراهم می کنند، دارای پسوند **AMD-V** هستند.

هنگام خرید CPU:

- **اگر قصد داشته باشیم CPU از نوع AMD برای کامپیوتری تهیه کنیم، باید بررسی کنیم که Mainboard موجود، سوکت AMD را پشتیبانی می کند یا خیر!**
  - CPU های نسخه های Ryzen 3 و 5 و 7 و 9 از سوکتی به نام AM4 استفاده می کنند.
  - CPU نسخه ی Thread ripper از سوکتی به نام TR4 استفاده می کند.
- **اگر قصد داشته باشیم CPU از نوع Intel برای کامپیوتری تهیه کنیم، باید بررسی کنیم و ببینیم که سوکت CPU مربوط به Mainboard موجود، از چه ورژنی می باشد. سوکت هایی مثل 1150 و 1151 و ... موجود می باشند.**
- **باید توجه کنیم که CPU موردنظر، از چه نوع RAM ای با چه ورژنی پشتیبانی می کند.**
- **هنگام خرید CPU باید به حداکثر میزان حافظه ای که برای RAM و Graphic Card و حداکثر کانالی که برای RAM های موجود پشتیبانی می کند نیز دقت کنیم:**
  - Max Memory Size
  - Max of Memory Channels : **هر دو درگاه یکرنگ Ram، یک کانال هستند.**
  - Graphic Video Max Memory

برای مقایسه ی دو CPU با هم: cpuboss.com

همه‌ی پردازنده‌ها به راحتی OverClock نمی‌شوند.

در مورد پردازنده‌های AMD، کار راحت‌تر است؛ اما Intel جزو شرکت‌هایی است که به ندرت اجازه‌ی Over clock را به کاربران می‌دهد.

با این حال، پردازنده‌هایی از این شرکت که پسوند X یا K دارند، مثل Intel Core i5-7600K قابلیت OC شدن را دارند.

توان پردازنده‌ها در تحمل سرعت‌های بالاتر با هم متفاوت است؛ حتی پردازنده‌هایی با مدل و مشخصات یکسان می‌توانند تحمل متفاوتی را نشان دهند. دلیل مشخصی برای این موضوع وجود ندارد و کاربران آن را با عنوان «شانس سیلیکونی» یاد می‌کنند.

- **هرچقدر پردازنده‌ی خود را به اجرای سریع‌تر وادار کنید، داغ‌تر می‌شود.**
- **یک Over clock پایدار، بین سرعت و گرما تعادل برقرار کند.**
- **اگر سیستم شما بیش از حد داغ شود، قبل از اینکه آسیبی ببیند به صورت خودکار خاموش خواهد شد.**
- **برای مقابله با حرارت یا خنثی کردن تاثیر آن، از قطعات خنک کننده و Fan و Thermal Paste استفاده می شود.**
- **اگر Thermal paste نزده باشیم، سیستم روشن باقی می ماند اما خطرناک است، اما اگر کلا CPU Fan را وصل نکرده باشیم، به محض کمی داغ شدن CPU، سیستم قطع یا خاموش می شود.**
- **خنک‌کننده‌های ارزان‌قیمتی که همراه اکثر CPU ها عرضه می‌شوند شاید به کار نیایند.**
- **باید Fan قوی تری تهیه کرد یا از خنک‌کننده‌های مایع، که عملکردی مانند رادیاتور ماشین دارند، استفاده کرد.**

- **بهترین نرم افزار جهت دریافت اطلاعات کامل سخت افزار سیستم، به خصوص CPU، نرم افزار CPU-Z می باشد:**
  - **در تب SPD، می توان اطلاعات سخت افزار نصب شده در هریک از Slot های Ram را مشاهده کرد.**

:(Random Access Memory) RAM

به نوع **RAM** های مورد استفاده برای **PC** ها، گفته می شود: **DIMM**
به نوع **RAM** های مورد استفاده برای **Laptop** ها، گفته می شود: **SODIMM**

- برای اطلاع از میزان و تعداد قابل پشتیبانی یک **Mainboard** از **RAM**، وقتی وارد **Option** ها و مشخصات آن می شویم، باید در قسمت **Memory** دقت کنیم.

- برای خنک کردن **RAM** ها، برروی آنها یک سینک قرار دارد که رنگی هستند.

- نصب **RAM** ها روی **Mainboard**، باید به صورت یکی درمیان باشد، که یک **Channel** را تکمیل کنند و سپس به **Channel** بعدی برویم.
  - به ازای هر **Channel** دو **Slot** وجود دارد.

- اولویت نصب در **Slot** ها، با **Slot** هایی است که نزدیکتر به **CPU** قرار دارند.
- اگر روی پایه های **RAM** خط خوردگی وجود داشته باشد، نشاندهنده ی این است که حداقل یکبار قبلاً نصب شده است.
- برای خطایابی **Ram**، از کنسول **Windows Memory Diagnostic** استفاده می شود.
- در مقایسه با یک سیستم **gaming**، سیستمی که به عنوان **Hypervisor** استفاده می شود، باید **Ram** قوی تری داشته باشد.

: Graphic Card

پردازنده ی کارت گرافیک **GPU** (**Graphics processing unit**) نام دارد.

شرکت های زیادی کارت گرافیک تولید می کنند، مثل **GeForce** و **Asus** و ... .
اما دو شرکت بزرگ سازنده ی **GPU**:

- **: Nvidia**

- **: AMD**

اگر یک کارت گرافیک جدید جایگذاری کردیم و پس از روشن کردن سیستم، هنگام **Boot** ، صدای بوق از کیس بیرون آمد، نشانه ی این است که **PSU** یا منبع تغذیه برای سیستم کافی نیست!

:(PSU) Power Supply Unit

وقتی دکمه ی پاور را می زنیم، اما سیستم روشن نمی شود به ترتیب راه های زیر را امتحان می کنیم:

1. وایرسیار و کابل برق کیس را چک می کنیم.
2. موس و کیبورد و اسپیکر و مانیتور را جدا کرده و دوباره تلاش می کنیم.
3. به آرامی درب کیس را باز کرده و کانکتورهای مربوط به **Power Switch** و همچنین مابقی را جدا می کنیم و توسط یک پیچگوشتی آن دو خار مربوط به **PowerSwitch** را به هم وصل می کنیم.
4. باطری **Mainboard** را جدا کرده و با یک پیچگوشتی، پایه ی موجود در جاباطری را به بدنه ی مجاورش متصل می کنیم که از تخلیه شدن برق درون آن مطمئن شویم و سپس دوباره باطری را سرجایش باز می گردانیم.
5. تمامی تجهیزات متصل به **Mainboard** را از آن جدا می کنیم، به جز کابل های **Power** که همچنان به آن متصل اند و دوباره امتحان می کنیم.
6. کابل های پاور را کاملاً از **Mainboard** هم جدا کرده و سپس در سوکت **20** یا **24** پینی **Power**، پین متصل به سیم سبز رنگ را به پین متصل به یکی از سیم های مشکی رنگ مجاورش، توسط یک قطعه سیم، متصل کرده و سعی می کنیم **Power** را روشن کنیم.
   - اگر باز هم روشن نشد، پس **Power** خراب است.
   - اگر روشن شد، باید بررسی کنیم و ببینیم که میزان برق خروجی آن صحیح و کافی است یا خیر.

   - اگر تست **Power** موفقیت آمیز باشد، پس یا **Mainboard** خراب است و یا **CPU**.

   برای بررسی اینکه آیا ایراد از **Mainboard** است یا **CPU**، کافی ست که اتصالات اولیه را دوباره وصل کنیم، اما اینبار یک **CPU** دیگر را جایگزین کنیم و تست کنیم، که اگر سیستم روشن شود، یعنی **CPU** خراب بوده است، و در غیراینصورت، اشکال از خود **Mainboard** است.

Secure Boot :

- **Secure Boot یکی از ویژگی های محیط UEFI می باشد.**
- **فرض کنید کسی باشد که یک Bootable DVD را که حاوی سیستم عامل Live** (اجرا بدون نیاز به نصب) **است را در دستگاه قرار داده و آن را بالا بیاورد! پس می تواند به سادگی به فایل‌های شخصی شما دسترسی پیدا کند! به همین جهت Secure Boot را فعال می کنیم.**
- **Secure Boot طوری طراحی شده تا malware ها (بدافزارها) در هنگام boot شدن سیستم، توانایی ایجاد اختلال نداشته باشند.**
- **وقتی secure boot را خاموش می کنیم، مثل این است که درب را برای ورود malware ها باز گذاشته ایم!**
- **همانطور که می دانیم، این امکان وجود دارد که Dual Boot را برای سیستم تنظیم کنیم که بتوان دو سیستم عامل را راه اندازی کرد، اما وقتی Secure boot را فعال می کنیم، این قابلیت Dual boot نیز قابل راه اندازی نخواهد بود. به همین جهت باید قابلیت Secure Boot را غیرفعال کنیم.**
- **همچنین وقتی که Secure Boot فعال باشد، دیگر نمی توان از طریق USB، سیستم را Boot کرد، که بتوان مثلاً نصب ویندوز از طریق USB flash را انجام داد.**

نکته: در صورت نیاز به استفاده از رسانه ای که Bootable باشد که در محیط BIOS کار می کند، علاوه بر Secure Boot نیاز است که قابلیت UEFI را نیز بر روی سیستم موردنظر، خاموش کنیم تا بتوان آن را بالا آورد، مثل DBAN که جهت Wipe کردن storage بکار می رود.

Network Expressions :

Baseband :

خط یا شبکه ای است که در یک لحظه، فقط یک سیگنال را از خود عبور می دهد.

Broadband :

خط یا شبکه ای است که در یک لحظه، بیش از یک سیگنال را از خود عبور می دهد. مثل کابل های مخابرات، **ADSL**، **VoIP** و ...

Broadcast :

Broadcast در معنای لغوی یعنی پخش کردن.

Broadcast کردن اطلاعات در شبکه، یعنی اینکه یک دستگاه (فرستنده) اطلاعاتش را به تمامی کامپیوتر های عضو آن شبکه ارسال کند.

به عنوان مثال، یک ایستگاه رادیویی، سیگنال هایش را به تمامی آنتن های گیرنده ی حاضر در محیط، می فرستد و آنتن ها از طریق سیگنال هایی که دریافت می کنند، می توانند تلویزیون مشاهده کنند.

به طور کلی ارتباط **Broadcast**، یک ارتباط یک به همه است.

- مثلاً یک دستگاه **WiFi-Modem** یا **Access Point**، با **Broadcast** کردن **SSID** خود، به شما این امکان را می دهد تا به شبکه ی **Wi-Fi** آن متصل شوید و از اینترنت استفاده کنید.
- مثلاً دستور **Ping** در **cmd** ، یک دستور **broadcast** است که بسته ای را به همه ی اعضای متصل به شبکه ارسال می کند تا بالاخره کامپیوتری که آن نام یا آدرس، مربوط به اوست، پاسخ می دهد.

Unicast :

فرض کنید یک تلفن دارید و یک شماره تلفن، شما این شماره را می گیرید و با شخص مورد نظر تماس برقرار می کنید. این ارتباط بین شما و شخص صاحب خط برقرار می شود و صحبت می کنید. کسی غیر از شما دو نفر از محتویات تماس با خبر نخواهد شد.

این نوع ارتباط، یک به یک یا **Unicast** نامیده می شود.

مثلاً زمانیکه شما یک صفحه **Website** را باز می کنید، وب سایت اطلاعات را ارسال می کند و شما از آن اطلاعات دریافت می کنید، و این هم یک ارتباط **Unicast** است.

حتی دانلود کردن یک فایل از یک **File Server** نوعی ارتباط **Unicast** است.

Multicast :

در این نوع ارتباط، یک کامپیوتر ارتباط خود را بصورت همزمان با چندین کامپیوتر دیگر برقرار می کند و شروع به ارسال و دریافت داده می کند.

در واقع زمانیکه صحبت از **Multicast** می شود، منظور گروهی مشخص از کامپیوترهاست که یک کامپیوتر با آنها ارتباط برقرار کرده است.

در **Multicast**، اطلاعات فقط به اعضایی منتقل می شوند که در آن گروه قرار دارند و اطلاعات به همه کامپیوترهای شبکه منتقل نخواهند شد.

دستگاه هایی که می خواهند اطلاعات مربوط به **Multicast** را دریافت کنند، بایستی به عضویت این گروه **Multicast** در بیایند.

حتما می دانید که کلاس **D** ، **IPv4** ، برای استفاده در موارد **Multicasting** است.

مثلاً توسط سرویس **WDS** در ویندوز **Server**، از روش **Multicasting** برای نصب **Windows** های تحت شبکه استفاده می کنیم.

: Bandwidth

میزان اطلاعاتی که در یک لحظه، به شکل علمی و تئوری قادر به عبور از خط ارتباطی هستند را بر حسب Hertz مشخص می کند.

: Throughput

میزان اطلاعاتی که به شکل واقعی و عملی، قادر به عبور از خط ارتباطی هستند را مشخص می کند.

: CrossTalk

به تاثیر سیگنال های الکتریکی یک کابل، بر روی یک کابل دیگر، crosstalk می گویند.

: Meta data

بجز محتوای یک فایل، و تنها بخشی از آن که حاوی مشخصات آن فایل است، بخش Meta data نامیده می شود.

نکات:

- بهترین شیوه ی نامگذاری کامپیوترهای عضو شبکه، استفاده از Asset ID و Mac address آنهاست.
- وقتی که Diagram مربوط به Topology یک شبکه را طراحی می کنیم، باید دو مورد زیر را حتماً در کنار هر دستگاه درج کنیم:
  - لیست آدرس های IP هر دستگاه
  - لیست Port های آنها همراه با وضعیت اشغالشان را

External Devices:

Network Interface Card (NIC) :

انواع NIC از نظر اتصال به PC :

- Slot board: روی main board نصب می شود.
- Onboard : بر روی main board به شکل بخشی از آن، تعبیه شده است.
- USB : مثل یک قطعه ی جانبی به پورت USB سیستم متصل می شود.
- SD Card

و هریک از همه ی این انواع NIC، شامل دو حالت wireless و wired نیز می باشند.

- به پورت‌های روی Router و Switch که Client ها به آنها متصل می شوند و به پورت NIC روی هر Client، پورت LAN یا پورت RJ45 گفته می‌شود.
- دستگاه‌هایی که دارای پورت RJ45 هستند، دستگاه‌های Ethernet-Ready نامیده می‌شوند.

دو استاندارد برای سرعت انتقال داده در پورت‌های LAN وجود دارد:

- Ethernet : دارای حداکثر سرعت تبادل ۱۰۰ مگابیت (تقریباً ۱۳ مگابایت) در ثانیه می باشد، که متوسط آن در عمل 8 MB/s است.
- Gigabit Ethernet (GbE): دارای حداکثر سرعت انتقال ۱ گیگابیت (تقریباً ۱۲۵ مگابایت) در ثانیه می باشد، که متوسط آن در عمل، 45 تا 80 MB/s است.

- از کابل Cat5e به بعد، همگی از استاندارد Gigabit Ethernet پیروی می کنند.

به عبارت دیگر انتقال اطلاعات یک CD (یعنی۷۰۰ مگابایت) از طریق یک اتصال Ethernet، تقریباً یک دقیقه طول می‌کشد، و انتقال همین میزان اطلاعات از طریق یک اتصال Gigabit Ethernet ، حدود 8 ثانیه زمان نیاز دارد.

نکته: سرعت یک شبکه، بر اساس کُندترین دستگاه متصل به آن شبکه تعیین می‌شود.
مثلاً اگر شبکه‌ای شامل چندین دستگاه، مسیریاب و کابل‌هایی با پشتیبانی از Gigabit Ethernet داشته باشیم و تنها یک اتصال Ethernet در این شبکه وجود داشته باشد، سرعت این شبکه حداکثر برابر با ۱۰۰ مگابیت در ثانیه خواهد بود.

: Router

- وقتی یک سرویس اینترنت خریداری می کنیم، **Internet-Service Provider** (ISP) به ما یک خط **DSL** اختصاص می دهد که با گیرنده ای به نام **DSL Modem** قابل اتصال خواهیم بود.
- **ISP**، طی بازه های زمانی متفاوت، آدرس های **IP** متفاوتی را به **DSL Modem** ای که دریافت کرده ایم، ارسال خواهد کرد.
  - می توانیم با پرداخت مقداری هزینه ی بیشتر، یک آدرس **IP** ثابت خریداری کنیم تا از هر محیط و شبکه ی متصل به اینترنت دیگر، به این مودم **DSL** دسترسی داشته باشیم.
- در حقیقت توسط این مودم **DSL**، فقط یک دستگاه، قادر به استفاده از اینترنت است.
- برای اینکه چند دستگاه قابلیت استفاده از این سرویس اینترنت را داشته باشند، نیاز به یک **Router** است تا بتوان اینترنت را بین همه ی دستگاه ها اشتراک گذاری کرد.

- **Router** دو سمت دارد، داخلی و خارجی!
- **Router** ارتباط همه ی دستگاه هایی که به سمت داخلیِ آن متصل شده اند را به شبکه ای که در سمت خارجیِ آن قرار دارد، یعنی اینترنت، برقرار می کند.
- برای سمت داخلی **Router**، بصورت دستی یک آدرس **IP** تعیین می کنیم که به آن **Gateway Address** هم می گویند.
- آدرس دستگاه های متصل شده ی داخلی هم باید در شبکه ی آدرس **Gateway Address** باشند.
- سمت خارجیِ **Router**، همان آدرس و مشخصاتی را خواهد داشت که از مودم **Internet** دریافت می کند. (**Public Address**)
- از بخش های مهم **Router** بخش **DHCP** است، که دیگر نیازی نیست تا بصورت دستی به دستگاه های داخلی، **IP** بدهیم.
- بخش مهم دیگر **Router**، بخش **Firewall** است. **Packet** هایی را که از خارج از شبکه می آیند، اگر هیچ یک از کاربران، آنها را درخواست نداده باشند، **Block** می کند.
- کاری که **Router** انجام می دهد، **routing** یا مسیریابی است (پیدا کردن و اختصاص دادن بهترین مسیر)، که این عملیات در **لایه ی سوم مدل OSI** یعنی **Network layer** انجام می شود.
- **Router** آدرس های **IP** دستگاه ها را در درون خودش در جدولی به نام **Routing table** ذخیره می کند.

DSL Modem and Router Connection:

در حقیقت، روی **DSL-Modem** خریداری شده، پورتی وجود دارد، به نام **Ethernet** و یا **Gigabit Ethernet**، و روی **Router** هم پورتی بنام **WAN** یا **GE** و یا **GE WAN**، به همراه چند پورت **LAN**.



برای اتصال **Modem** و **Router** ، باید پورت **Ethernet** روی **Modem** را به **WAN Port** روی **Router** وصل کنیم.
(البته بعضی **Router** های تجاری، شامل دو پورت **WAN** هستند که به کمک آن‌ها می‌توان در یک زمان، دو دسترسی مجزا به اینترنت را فراهم کرد.)
و پورت **DSL** روی **DSL-Modem** هم به خط تلفن وصل می شود.

همانطور که در تصویر **Router** می بینید، معمولاً **Router** ها و البته **managed Switch** ها، پورتی به نام **Console** دارند، که برای اتصال آن به یک کامپیوتر، جهت **config** کردن خود آن است. پس نیاز به نوعی کابل به نام **console cable** یا **Rollover cable** داریم. که به یکی از صورت های زیر می باشد:

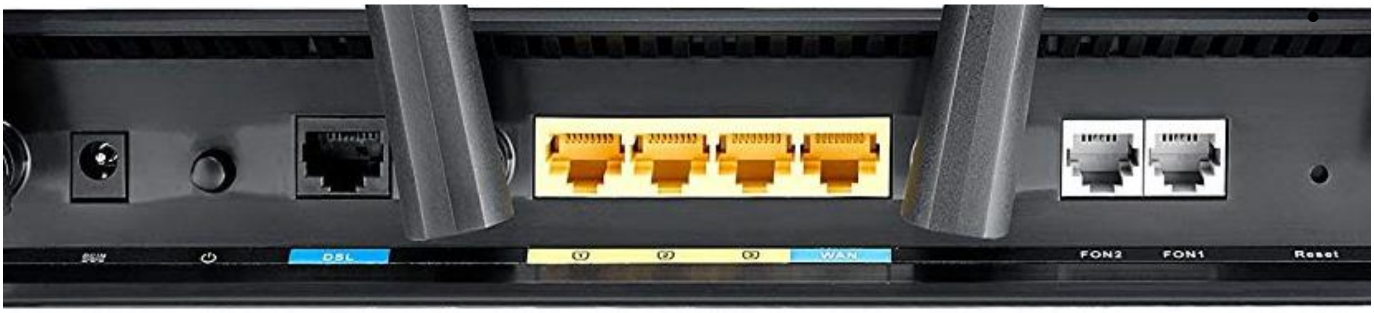




و اگر PC، دارای پورت سریال نبود، باید از آداپتور زیر، برای تبدیل و اتصال این کابل از Router به PC استفاده کنیم:



- مودم هایی هستند بنام Modem-Router، که هم مودم DSL هستند و هم Router.
- Modem Router ها هم دارای پورت WAN هستند و هم پورت DSL.



➢ Router Access Point :

امروزه Router های شرکت ها و اداره ها دارای WiFi نیز می باشند (خودشان نقش یک AP را نیز دارند)، و بطورمعمول برای آن، دو Profile تعریف می کنیم:

- **Staff Wifi** : که restricted یا محدود به دستگاه های پرسنل شرکت می باشد و معمولاً با Certicate یا mac filtering، امن شده و نیازی به پسورد جهت اتصال به آن نیست، چون هرکسی نمی تواند به آن متصل شود.

مگر اینکه پسورد این wifi-profile را فقط پرسنل شرکت داشته باشند؛ پس نیازی به certificate یا mac filtering نخواهد بود.

- **Guest WiFi** : که آن را public درنظر می گیریم و همه ی افراد می توانند از آن، جهت اتصال به اینترنت استفاده کنند، اما هیچ اتصالی به شبکه ی داخلی شرکت نخواهند داشت؛ و دو حالت دارد:
  - **Private** : جهت اتصال به آن، نیاز به Password است.
  - **Public** : نیاز به هیچ رمزعبوری ندارد.

- از آنجا که نوع انتشار سیگنال های Router به شکل کروی می باشند، بهتر نقطه برای قرار گیری آن در یک ساختمان یا خانه، مرکز خانه است.
- یکی از راه های حفظ امنیت Router ها، این است که ابتدا default credential ورود به تنظیمات Router را تغییر دهیم، سپس firmware آن را update کنیم.

Switch and Hub :

- از نظر فنی، می‌توان بدون استفاده از Router یا Switch و به کمک یک کابل، دو رایانه را به هم متصل کرده و یک شبکه ایجاد کرد. اما استفاده از این شبکه مستلزم تنظیم و پیکربندی دستی IP آدرس‌ها است که زمانبر خواهد بود.
- به کمک Hub و Switch می‌توان تعداد دستگاه‌های Ethernet-Ready در یک شبکه را افزایش داد.
- Hub بصورت Broadcast کار می کند.
- Switch بصورت Multicast کار می کند.
- تفاوت اصلی میان هاب و سوئیچ این است که هاب از یک کانال اشتراکی (Shared Channel) برای تمام پورت‌های خود استفاده می کند، چیزی مشابه به Bus Topology، در حالیکه که سوئیچ برای هر پورت خود یک کانال اختصاصی (Dedicated) دارد.
- پس هر چه تعداد Client های Hub افزایش پیدا کند، سرعت (Data transfer rate) آن کاهش می‌یابد، در حالیکه تعداد کاربران متصل به یک سوئیچ، در نرخ تبادل اطلاعات آن تغییری ایجاد نمی‌کنند، به همین دلیل Hub ها بسیار ارزانتر از سوئیچ ها هستند.
- Hub در لایه ی اول یعنی Physical layer کار می کند و از معایب آن، هدر رفتن حجم زیادی از پهنای باند است.
- چون سوئیچ در لایه ی دوم یعنی data-Link layer کار می کند، که در این لایه، آدرس IP تعریف نشده است، همه ی ارتباطات بر اساس Mac Address انجام می شوند.
- نوع Connection هم در Switch و هم در Router بصورت Full Duplex می باشد، اما در Hub بصورت Half Duplex است.
- Router از آدرس IP برای انتقالات و دریافت ها استفاده می کند و Switch از Mac Address استفاده می کند، و Hub از هیچ مشخصه ای استفاده نمی کند.
- Switch های جدید، لایه ی سوم (Network layer) را نیز پشتیبانی می کنند که این باعث می شود تا علاوه بر عملیات Switching، درست مثل یک Router، عملیات Routing بین شبکه ها را نیز انجام دهند.

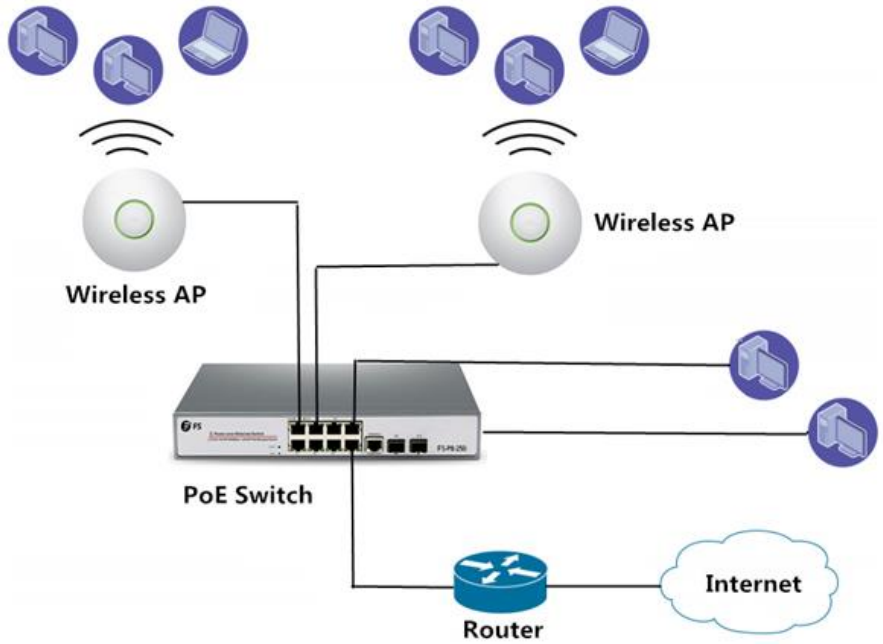
- اگر تعداد Client های شبکه از تعداد پورت های روی Router بیشتر شود، و یا فاصله ی چند Client که در کنار هم قرار دارند، با Router خیلی زیاد شود، نیاز به تهیه ی Switch خواهیم داشت.
- بطورکلی، از Switch و Hub برای اتصال دو یا چند PC یا هر دستگاه دیگر به یک شبکه استفاده می شود، اما از Router برای اتصال دو یا چند شبکه به هم استفاده می شود.

- همیشه تعداد سیستم هایی که توسط یک سوئیچ می توانند به شبکه متصل شوند، به اندازه ی تعداد پورت های سوئیچ، منهای یک می باشند. چرا که یکی از پورتهای سوئیچ، برای اتصال سوئیچ به شبکه ی اصلی استفاده می شود. البته اگر شبکه ی دیگری وجود نداشته باشد!
- تنها دستگاهی که می تواند یک User از یک VLAN را قادر به برقراری ارتباط با یک User از یک VLAN دیگر کند، Router می باشد.

PoE Switch :

فرض کنید که مودم یا مسیریابی داریم که فاقد قابلیت WiFi است، یا اینکه در شبکه مان، در فاصله ای دورتر از Access Point اصلی شبکه مان، دریافت سیگنال WiFi امکانپذیر نیست، در این حالات برای انتشار سیگنال شبکه در محیط، کافی ست از یک Access Point دیگر استفاده کنیم.

اگر Access Point جدید، قابلیت POE هم داشته باشد، بهتر و تمیزتر خواهد بود.



فرض کنیم Access Point مان POE باشد، اما Switch یا Router مورد نظر، POE نباشد! دو راهکار خواهیم داشت:

- یک آداپتور برق برای Access Point تهیه و مثل AP های معمولی آن را وصل کنیم.
- یک POE Injektor بین راه اتصال سوئیچ و Access Point قرار دهیم.

➢ POE Injektor :

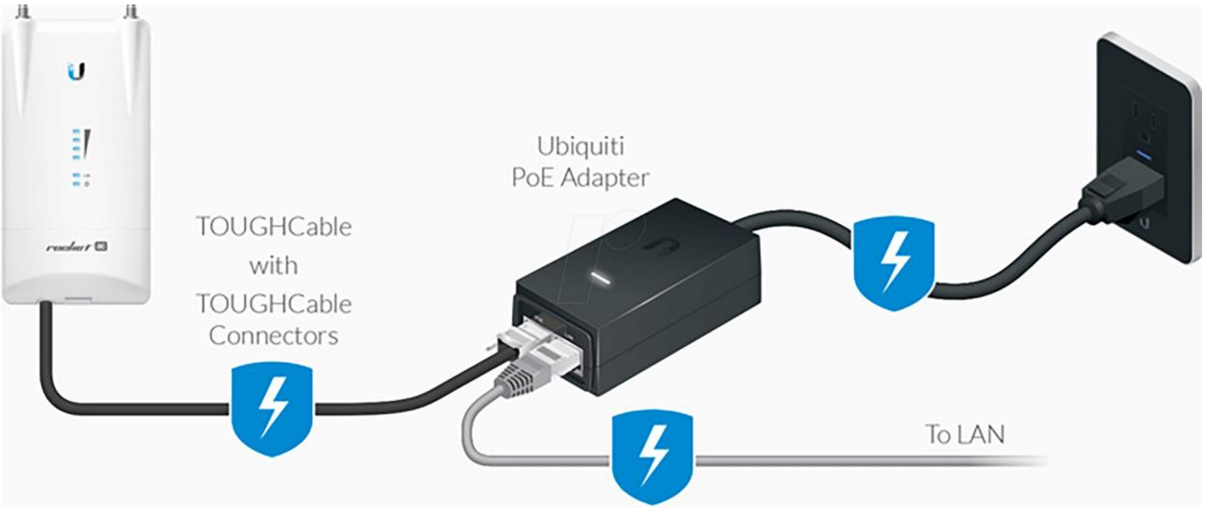
وقتی که بخواهیم یک دوربین یا تلفن یا Access Point یا هر قطعه ای که فقط از طریق POE کار می کند را به شبکه ای وصل کنیم که سوئیچ آن POE نیست، نیاز به قطعه ای کوچک داریم به نام POE Injektor، که از طریق دوشاخه اش به پریز برق متصل می شود و در طرف دیگرش، دارای دو پورت POE و LAN می باشد.

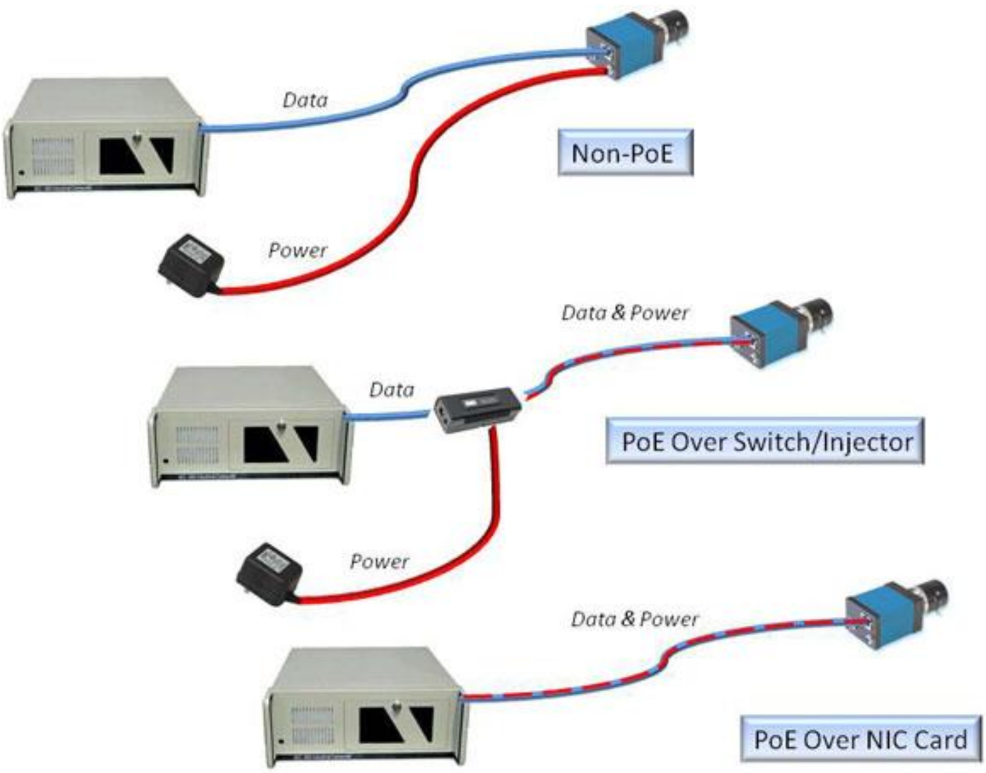
- پورت POE را به دستگاه POE مورد نظر وصل می کنیم.
- پورت LAN را به سوئیچ شبکه وصل می کنیم.



اصولاً برای اتصال یک Access Point به شبکه، از کابل شبکه استفاده می شود، اما اگر این فاصله زیاد بود، یا کابلکشی و نصب و اتصال آن، نیاز به صرف زمان و هزینه باشد، می توان از **Power Line** (Ethernet over power) استفاده کرد.

POE Injektor ها اشکال مختلفی دارند، که شکل بالا و شکل زیر، از انواع رایج آن هستند:

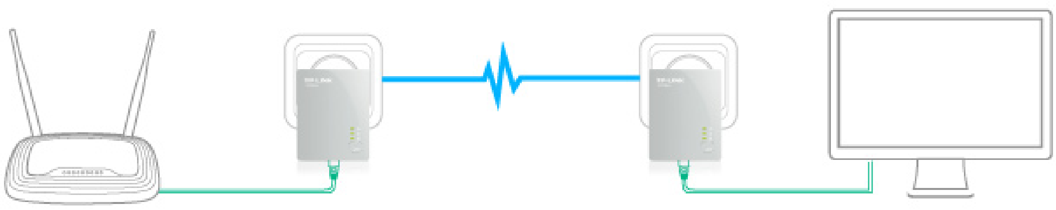




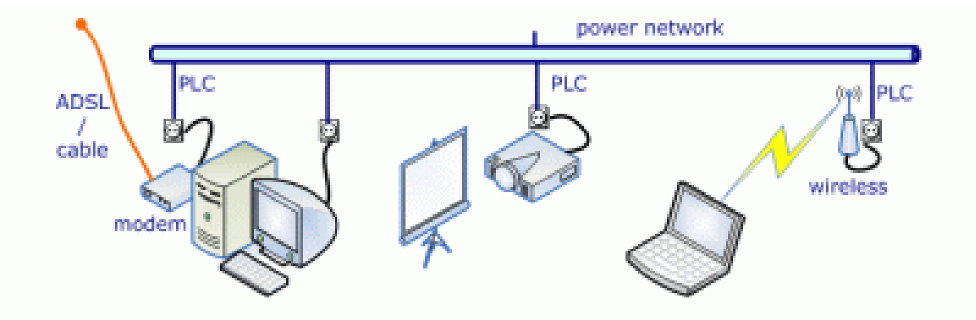
: (Power-Line Communication) PLC

- خطوط برق شهری دارای ولتاژ 220 V و فرکانس 50 Hz می باشند و ما صرفا همین استفاده را از خطوط برق می کنیم.
- تکنولوژی Power Line محصولی است که امکان اتصال کامپیوترهای یک ساختمان را بدون نیاز به کابل‌کشی شبکه و فقط با استفاده از سیم‌کشی برق آن ساختمان، فراهم می‌سازد.
- هر آداپتور Power Line، از سیم کشی برق خانه، به عنوان یک شبکه ی Data استفاده می کند و درگاه های Ethernet را به پریزهای برق متصل می کند.
- در حقیقت الکتریسیته ی موجود در سیم‌ها، تنها از یک فرکانس استفاده می‌کند، همانند یک ایستگاه رادیویی که تنها از یک موج خاص استفاده می‌کند. در این طیف، فضای کافی برای سایر ایستگاه‌ها وجود خواهد داشت.
- سرعت آداپتورهای Power Line بر اساس مدل آنها متغیر است.
- برای استفاده از این شبکه، کافی ست که دستگاه Ethernet-Ready را توسط یک کابل شبکه، به آداپتور PLC وصل کنید، و سپس آداپتور را وارد پریز برق کنید.

فرض کنید بخواهیم یک لپ تاپ را توسط Power Line به یک سوئیچ یا مودم روتر، که در اتاقی دیگر است، وصل کنیم.
ابتدا هم سوئیچ و هم لپتاپ را توسط یک کابل شبکه، بطور جداگانه به آداپتورهای PLC شان وصل کرده و به پریز برق متصل می کنیم.

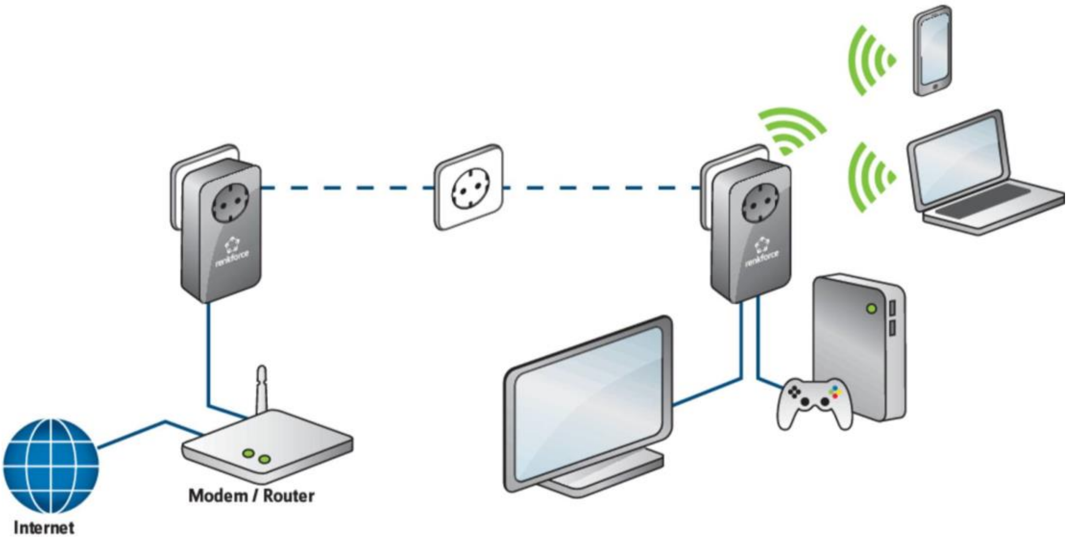


- سپس وقتی دکمه ی pair روی یکی از طرفین را فشار دادیم، دو دقیقه فرصت داریم تا دکمه ی pair روی آداپتور دیگر را نیز فشار دهیم تا پس از مدت کوتاهی اتصال برقرار شده و چراغ برقراری اتصال روی هردو آداپتور روشن شود.
- پس برای اتصال هر دستگاه به شبکه، نیاز به یک آداپتور PLC خواهد بود.



نکته: با بکارگیریِ این دستگاه، امکان انتقال اطلاعات فقط بر بستر شبکه ی برق بسته (سیم‌کشی که از کنتور برق شروع شده و به خود همان کنتور ختم شود) فراهم می شود.

- بسته به اینکه آداپتور PL چند پورت LAN داشته باشد، می تواند تعدادی دستگاه Ethernet-Ready را وارد شبکه کند.
- برخی PL ها قابلیت Wlan نیز دارند، یعنی Client ها بدون اتصال کابلی، می توانند بصورت WiFi به آنها وصل شده و وارد شبکه شوند.



همانطور که در شکل می بینید، PL سمت راست، دو دستگاه را بصورت کابلی و دو دستگاه را بصورت Wlan وارد شبکه کرده است.

- مزیت استفاده از Power Line ، امکان ایجاد شبکه در ساختمان‌هایی است که عملیات کابل‌کشی در آن دشوار است یا دسترسی به تمام نقاط آن ساختمان ممکن نیست.
- دستگاه‌های Power Line می‌توانند تا طول ۳۰۰ متر از شبکه‌ی برق ساختمان را به عنوان محیط انتقال داده ها استفاده کنند.
- به همین سادگی از Power Line ها به عنوان جایگزینی برای Wi-Fi یاد می شود.
- بهتر است که Power Line به پریزهایی متصل شود که از دستگاه‌هایی چون یخچال، لباسشویی و مایکروفر فاصله مناسبی دارند.

Managed Switchs :

برای ورود به صفحه ی تنظیمات یک Modem یا Router یا Switch باید PC یا Labtop ای که با آن وصل می شویم، دارای رنج IP یکسانی با Switch یا Router داشته باشد؛ به عبارتی در یک شبکه قرار گرفته باشند.
یعنی حتی اگر Labtop و Switch به شکل کابلی و مستقیم هم به هم متصل باشند، اگر دارای محدوده و کلاس IP یکسان نباشند، هیچ تماسی بین شان برقرار نمی شود. پس نمی توان صفحه ی User Interface دستگاه را باز کرد.
چون اتصال سخت افزاری برقرار است، اما اتصال نرم افزاری شان هنوز بی معنی ست.

اگر DHCP از قبل در دستگاه، فعال بوده باشد، به محض اتصال Labtop، دستگاه بطور خودکار یک IP به Labtop اختصاص می دهد، و ارتباطشان برقرار می شود.
اما اگر DHCP در آن فعال نباشد، باید در Labtop وارد تنظیمات Network شد، و بصورت manuall یک IP در کلاس IP آن دستگاه تعیین کرد.

- IP های پیشفرض رایج در Switch های D-Link: 192.168.1.1
- IP های رایج در مودم های FritzBox:
  192.168.178.1

بطور معمول، وقتی DHCP در سوئیچ یا مودم خاموش باشد یا دچار مشکل باشد، احتمال آن است که PC متصل شده به آن، یک آدرس APIPA دریافت کند، که دو حالت خواهیم داشت:

- اگر IP دستگاه را داریم، باید IP سیستم را بصورت manually در رنج و محدوده ی IP آن تعیین کنیم تا به دستگاه متصل شده و بتوانیم صفحه ی تنظیمات آن را باز کنیم.
- اگر IP دستگاه را نداشته باشیم، مجبور به reset کردن آن خواهیم بود.

اما اگر دستگاه متصل شده، یک switch است که بخشی از یک شبکه ی بزرگتر است، باید به DHCP Server مراجعه کرد تا IP اختصاص داده شده به آن را پیدا کنیم.

- فرض کنید که یک Router و یک Labtop داریم، و می خواهیم وارد صفحه ی تنظیمات Router شویم.
- IP روتر 192.168.12.1 می باشد.
- اما DHCP در Router روشن نیست.
- راه حل این است که بصورت دستی برای لپتاپ، یک IP تعیین کنیم، اما همکلاس با کلاس Router یعنی 192.168.12.X

همانطور که می دانید، دستگاه هایی که به سوئیچ PoE متصل می شوند، نیازی نیست که بطورحتمی از تکنیک PoE پشتیبانی کنند. به همین جهت، این سوئیچ ها، دارای دو mode هستند:

❖ Link/Act Mode :

- **برای پورت های معمولی و پورت های SFP:**
  - چراغ سبز ثابت: اتصال و آماده بکاریِ دستگاه متصل شده به پورت را نشان می دهد، چه PoE باشد، چه Non-PoE.
  - چراغ سبز چشمک زن: به معنای انتقال ترافیک شبکه با سرعت 1 گیگابیت یا 1000 مگابیت در ثانیه است.
  - چراغ نارنجی چشمک زن: به معنای انتقال ترافیک شبکه با سرعت 10 تا 100 مگابیت در ثانیه است.

- **برای پورت های +SFP :**
  - چراغ سبز چشمک زن: به معنای انتقال ترافیک شبکه با سرعت 10 گیگابیت یا 10000 مگابیت در ثانیه است.
  - چراغ نارنجی چشمک زن: به معنای انتقال ترافیک شبکه با سرعت 1 گیگابیت در ثانیه است.

❖ PoE Mode :

- چراغ سبز ثابت: اتصال و آماده بکاری دستگاه PoE متصل شده به پورت را نشان می دهد.
  در حقیقت، این mode فقط برای مشخص کردن دستگاه های PoE متصل شده می باشد.

- در برخی سوئیچ ها، در صورت استفاده از دو یا چهار پورت سمت راستی که SFP هستند، اجازه ی استفاده از پورت های معمولی را نخواهیم داشت. یعنی اگر یکی از SFP ها مشغول شود، حداقل یکی از پورتهای معمولی باید خالی بماند.

در حالی که در برخی سوئیچ ها اینچنین محدودیتی وجود ندارد، و همه ی پورتها به شکل همزمان می توانند استفاده شوند.

- اگر در جلوی سوییچ، نمایشگر کوچکی بنام Stack ID قرار داشت، نشاندهنده ی این است که این سوییچ قابلیت stack شدن را دارد، یا به عبارتی stackable است، و این شماره، نشاندهنده ی شماره ی این سوییچ در مجموعه ی Stack است.



یکی از قابلیت های Switch های D-Link ایجاد برنامه ریزی های زمانی مختلف برای خاموش یا غیرفعال کردن سه ویژگی مرتبط به سوئیچ در بازه های زمانی مختلف است.

در صفحه ی UI ، در منوی سمت چپ:

ابتدا در گزینه ی Time Profile بازه های زمانی مورد نظرمان را با نام های دلخواه، تعریف و ذخیره می کنیم.

سپس در بخش Power Saving، می توانیم برای هریک از سه گزینه ی زیر، دو time profile را در نظر بگیریم، تا در این بازه های زمانی، آن گزینه قطع یا خاموش شود.

- LED Shut-off : خاموش کردن چراغ های مربوط به تک تک پورت ها.
- Port Shut-off : قطع کردن ارتباط داده ای تک تک پورت ها.
- System Hibernation : قطع کردن مصرف برق تک تک پورت ها.

➢ ARP (Address Resolution Protocol) :

بطور خلاصه، **ARP**، پروتکل تبدیل کننده ی آدرس **IP** به آدرس **Mac** است.

نکته: ARP فقط مختص به شبکه های **IP ورژن چهار (IPv4)** می باشد.

همانطور که می دانیم، در لایه ی دوم **OSI**، توسط **Mac Address** سیستم ها شناخته شده و با آنها ارتباط برقرار می شود و در لایه ی سوم، توسط **IP**.

Mac Address یک آدرس **48** بیتی است که در قالب **6** جفت اعداد در مبنای **16** (هگزا دسیمال)، توسط شرکت سازنده ی هر دستگاه، برای آن طراحی و ثبت و درج می شود.

_____:_____:_____:_____:_____:_____

درحقیقت تمامی ارتباطات در بخشی از یک شبکه ی **Lan** که تحت یک **Switch** کار می کنند، بر اساس **Mac Address** می باشند، اما به محض نیاز به ارتباط با یک سیستم که تحت کنترل اولین **Switch** متصل شده نیست، پروتکل **ARP** که به صورت **Broadcast** عمل می کند، آدرس **MAC** مقصد موردنظر را، که **IP** آن را داریم، پیدا می کند.

به عبارت دیگر، **در میان دو لایه ی Network و Datalink، پروتکلی وجود دارد به نام ARP** که ارتباط میان **Mac Address** ها و **IP Address** ها را هماهنگ می کند.

پروتکل **ARP** در هر یک از سیستم های عضو شبکه و همچنین در هر **Switch** وجود دارد که شامل جدولی ست بنام **ARP Table**.

- **در سیستم های Client، به سادگی و با درج arp -a در cmd می توان محتویات این جدول را مشاهده کرد.**

در این جدول، **IP** ها و **Mac Address** های همه ی سخت افزارهایی که با این عضو در ارتباط هستند، ذخیره شده اند.

یکی از کاربردهای این پروتکل زمانی ست که در یک شبکه، **PC1** قصد دارد با **PC2** که فقط آدرس **IP** آن را دارد، ارتباط برقرار کند.

خب این ارتباط برقرار نمی شود، چون در لایه ی دوم، چیزی به نام **IP** معنی ندارد، و همچنین ما **MAC Address** مربوط به **PC2** را نداریم!

این یعنی اینکه **ARP Table** ناقص است!

پس به این شکل عمل خواهد شد:

1. **PC1** یک بسته ی **ARP** ، شامل **IP** مقصد مورد نظرش می سازد و بصورت **broadcast** در شبکه ارسال کرده و درخواست می کند که کسی که دارای این **IP** است، پاسخی ارسال کند. این بسته، **ARP Request** نامیده می شود.

- **Arp Request** تا زمانی که به یک شبکه ی دیگر نرسیده باشد (**VLAN** یا **Router** یا **Subnet**)، مدام پیش رفته و به همه می رسد.
- **Arp Request** که در لایه ی دو انجام می شود، توسط یک **broadcast Mac Address** ارسال می شود: **FF:FF:FF:FF:FF:FF**

2. وقتی **Arp Request** به دست **PC2** برسد، او هم یک بسته به **PC1** پس می فرستد که این بسته **ARP Reply** نامیده می شود.

- حال که مشخصات **PC2** به **Arp Table** اضافه شده است، از این به بعد ارتباطات از محدوده ی **PC1** با سیستم **PC2**، بصورت **Unicast** خواهد بود.
- در واقع این پروتکل و فرآیند هایش درون **Switch** عمل می کنند. یعنی سوئیچ از طرف **PC1** بسته ای را ارسال می کند.

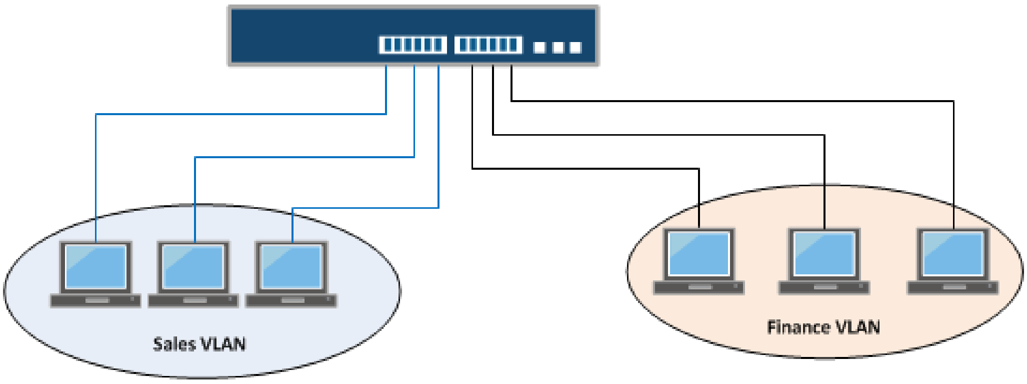
نکته: این احتمال وجود دارد که پس از مدتی، آدرس IP برخی Client های شبکه، تغییر کرده باشند. پس می توانیم Arp Table را یکبار پاک کنیم تا از نو پر شود: arp -d

➢ VLAN (Virtual Local Area Network) :

- سوئیچ ها روشی مطمئن و سریع برای مبادله ی اطلاعات بین گره ها در یک شبکه را فراهم می نمایند.

اما با اینحال همزمان با رشد شبکه و افزایش تعداد ایستگاهها و سرویس دهندگان، شاهد بروز مشکلات و پیچیدگی های ارتباطی خواهیم بود، پس قابلیتی پدید آمد که توسط آن، بسیاری از سوئیچ های شبکه حذف و عملکرد همه ی آنها در یک سوئیچ خلاصه شد.

- در حقیقت، VLAN قابلیتی ست که به سوئیچ ها اضافه شده است، و اگر سوئیچی قابلیت VLAN را پشتیبانی نکند، قادر به ایجاد VLAN نخواهیم بود.
- هر یک VLAN که بر روی سوئیچ ایجاد می گردد، مثل یک شبکه ی مجزا با سوییچی متفاوت عمل خواهد کرد.



در شکل بالا، با استفاده از قابلیت VLAN بر روی سوئیچ، دو VLAN ایجاد شده است که به هر یک سه Client متصل شده اند.

توسط Vlan ها:

➢ شاهد کاهش چشمگیر هزینه های برپایی یک شبکه خواهیم بود.

❖ وقتی یک Node، یک BroadCast Packet ارسال می کند، این Packet به نزدیکترین Switch رسیده و پخش می شود، اما این پخش شدن به پایان نمی رسد، بلکه به Switch های بعدی رفته و باز هم پخش می شود، این پخش شدن تا زمانی که به یک Router نرسد، در هر رسانه ی انتقالی که باشد و تا هرکجایی که شبکه امتداد پیدا کرده باشد، ادامه خواهد یافت، که این باعث ایجاد یک ترافیک بی معنی در شبکه می شود. پس به جز بکارگیری یک Router، تنها می توان دست به VLan بندی Switch زد.

❖ زمانی که ایستگاه شماره یک متعلق به VLAN1، یک پیام Braodcast را ارسال می نماید، سوئیچ، آن را فقط برای End Device های با آدرس مشابه که در خود VLAN1 قرار دارند، می فرستد و End Device های متعلق به VLAN2، هیچ اطلاعی از این پیام Broadcast دریافت نخواهند کرد.

➢ امنیت افزایش پیدا خواهد کرد. (همراه با انجام Port Security):

مثلاً ایجاد یک Vlan خاموش برای پورت های بی استفاده ی Switch.

فرض کنید بخواهیم زیر ساخت شبکه ی موجود در یک سازمان بزرگ را به دوازده شبکه ی جداگانه تقسیم کنیم.
پس می توان با تهیه ی دوازده Switch و اتصال ایستگاههای مورد نظر به هر یک از آنان، این کار را انجام داد؛ و یا اینکه توسط یک یا چند سوئیچ که قابلیت VLAN را پشتیبانی می کنند، آن را انجام داد.

در زمان ایجاد VALN، می باید تمام End Device ها را به سوئیچ متصل و در ادامه، ایستگاههای مرتبط با هر VLAN را مشخص کرد.

کاربردهای VLAN :

- User هایی که به High-Security نیازمندند را می توان در یک VLAN تعریف کرد که ارتباطشان با سایر اعضا قطع باشد.
- Traffic شبکه به نحو قابل توجهی کم شده و Broadcast-Storm (ترافیک شدید ناشی از هجوم ترافیک های عادی) حذف می شود.

فرض کنید که یک Switch-A را Vlan بندی کرده ایم که دارای Vlan 1 و Vlan2 و Vlan3 می باشد.
اگر این Switch-A را به Switch-B که دقیقا او هم دارای سه Vlan می باشد متصل کنیم:

- پورت ها یا درگاه های VLan1 در Switch-A ، پورت های VLan1 در Switch-B را شناسایی کرده و قابل تماس با هم هستند.
- پورت های VLan2 در Switch-A ، پورت های VLan2 در Switch-B را شناسایی کرده و قابل تماس با هم هستند.
- پورت های VLan3 در Switch-A ، پورت های VLan3 در Switch-B را شناسایی کرده و قابل تماس با هم هستند.

- اگر Switch-A را به Switch-C که Vlan بندی نشده است، متصل کنیم:

پورت های Switch-C فقط می توانند پورت های VLan1 در Switch-A را شناسایی کرده و ارتباط برقرار کنند.
چون در حالت پیشفرض همه ی پورتهای همه ی Switch ها، در Vlan1 قرار دارند.

نکته:

- به Vlan1، در اصطلاح، Native Vlan هم گفته می شود.
- این قابلیت وجود دارد که Native VLan را تغییر داد.
- از آنجایی که لازم است که بعد از اولین راه اندازیِ VLan های یک Switch، Native VLan را تغییر داد، بهترین کار این است که پورتهای بی استفاده و خاموش Switch را در Native VLan قرار داد.

➢ Switch Modes :

1. Access Mode :

پورتهای معمولی که برای ارتباط **Switch** با **End Device** ها (PC, Printer, Labtop, …) بکار می رود.
در این **Mode**، بسته ها بصورت **Untag** یا بدون برچسب (**Tag**) ارسال و دریافت می شوند.

2. Trunk Mode :

- پورتهایی هستند که برای ارتباط دو **Switch** با یکدیگر بکار می روند.
- در این **Mode**، بسته های ارسالی، در درگاه **Trunk** یک **Tag** دریافت کرده و سپس ارسال می شوند و بسته های دریافتیِ دارای **Tag**، در درگاه **Trunk** بررسی شده و **Tag** شان خوانده می شود.
- در **Switch** های دارای **Vlan**، به پورتهای **Native Vlan**، هیچ **Tag** ای اضافه نمی شود.
- با انجام تنظیمات، می توان مشخص کرد که کدام **Vlan** ها بتوانند از درگاه **Trunk** خارج شده و کدام نتوانند.
- درگاه **Trunk**، قابلیت حمل همزمان بسته های چند **Vlan** را دارد.

- درگاه **Trunk**، از دو پروتکل استفاده می کند:
  - **Inter-Switch Link-ISL :**
    - مخصوص دستگاه های **Cisco** می باشد.
    - **26 Byte** برای **Tag** یا **Header**، به بسته اضافه می کند، که در زمان دریافت، حذف می شود.
  - **802.1Q :** پروتکل استاندارد درگاه های **Trunk** می باشد.
    - **4 Byte** برای **Tag** یا **Header**، به بسته اضافه می کند، که در زمان دریافت، حذف می شود.

3. Dynamic Mode :

در این **Mode**، درگاه ارسال کننده، به شکل اتوماتیک با درگاه مقصد هماهنگ (مذاکره) می کند و یکی از دو **Mode** دیگر را انتخاب می کند.

: Power Support

دو اصطلاح در مورد مشکلات الکتریکی وجود دارند:
Blackout: به معنای خاموشی کامل می باشد. یعنی زمانی که برق، بطورکامل قطع می شود.
Brownout: به معنای خاموشی موضعی و یا تا حدی کم شدن شدت برق می باشد.

همانطور که می دانیم، گاهی هم جریان برق، دچار نوسانات (کم و زیاد شدن) **ناگهانی می شود که به آن Electrical oscillations گفته می شود.**

جهت پشتیبانی از جریان برق، سه دستگاه وجود دارند:

➢ Battery Backup:

Battery Backup که البته با نام Power Bank هم شناخته می شود، دستگاهی است که پس از اتصال به لوازم کامپیوتری، در صورت رخ دادن brownout یا blackout، فوری وارد عمل شده و از قطع شدن برق موردنیاز دستگاه و همچنین آسیب ناشی از نوسانات برق جلوگیری کند.

➢ Surge protector:

این دستگاه که آن را با نام محافظ برق نیز می شناسیم، جهت مقابله با نوسانات برق و حفظ یکدستی جریان برق ورودی به دستگاه متصل شده استفاده می شود، که کم و زیاد شدن امواج الکتریسیته را خنثی می کند.
و این دستگاه، حداقل ترین و ارزان ترین راهکار در برابر نوسانات الکتریکی می باشد.

➢ UPS (Uninterruptible Power Supply):

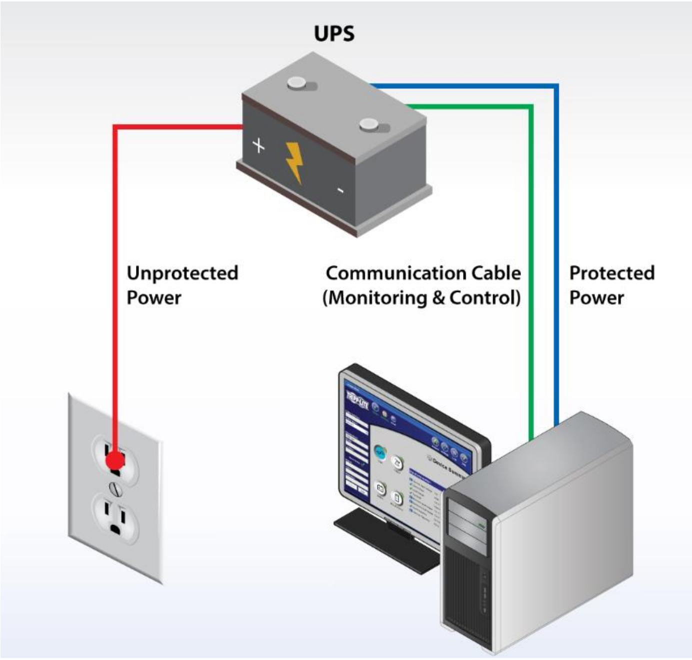
یک سری دستگاه ها در شبکه وجود دارند، که باید تا جای ممکن تلاش کنیم که هیچگاه برق آنها قطع یا دچار ضعف نشود، و در صورت طولانی مدت شدت قطعی، این دستگاه ها، به شکل مناسب و هماهنگ شده، خاموش شوند، طوری که هیچ Data ای از بین نرود.
مثل Server، Router و ...
UPS خودش دارای Battery است و علاوه بر توانایی های Battery Backup و Surge protector، قدرت و کارایی بیشتری هم نسبت به آنها داشته و برای پشتیبانی از دستگاه های مهمی مثل Server استفاده می شود.

بطورمعمول، دستگاهی که باید zero down time داشته باشد را به UPS و یا Battery Backup متصل می کنیم.
مثلاً هم Server و هم Router باید توسط UPS، پشتیبانیِ برقی (power support) **داشته باشند.**

درحقیقت UPS را می توان مشابه یک وایرسیار فرض کرد!

علاوه بر کابل برق خودش (Power connection) که جهت تأمین برق خودش، به پریز برق وصل می شود، تعدادی درگاه مادگی، برای اتصال کابل برق دستگاه های دیگر، به خود **UPS** وجود دارند. (بطور مرسوم هشت عدد یا بیشتر)

- با توجه به اینکه **Server** ها، حداقل دو درگاه اتصال کابل برق دارند، بطورمعمول، یکی از آنها را به **Server** و دیگری را به پریز برق معمولی وصل می کنیم. در صورت قطعی برق پریز، **Server** همچنان روشن می ماند، چرا که برق مصرفی اش را از خود **UPS** دریافت می کند، پس حداکثر استفاده را می کند تا یک **Shutdown** صحیح را اجرا کند.
- اما بطورمعمول، یک درگاه **USB** هم بر روی **UPS** وجود دارد، که جهت اتصال **Server** به **UPS**، علاوه بر کابل برق، یک اتصال **data** هم توسط یک کابل **USB** و این درگاه، استفاده می شود.



- اتصال این کابل داده، جهت گزارش گیری و اطلاع دادن به **Server** است. مزیت این گزارش گیری ها و اطلاعیه ها، این است که پس از قطع شدن احتمالی برق، **Server** را همچنان، جهت نگه داشتن و ذخیره کردن سرویس ها روشن نگه داشته، و آماده ی یک خاموشی صحیح خواهد کرد؛ و از خاموش شدن ناگهانیِ آن جلوگیری می کند. البته بجای این کابل **USB**، همچنین می توان از یک کابل با سوکت موازی یا سریال که درگاه آن در کنار درگاه **USB** روی **UPS** قرار دارد، هم استفاده کرد.
- با توجه به اینکه، **UPS** مورد استفاده در شبکه ی اداره های کوچک، قدرت زیادی ندارند که **Server** را برای ساعت ها روشن نگه دارد، پس به محض قطع شدن جریان برق اصلی، شروع به اجرای فرآیندهای لازم جهت **Shut down** می کند.
- باید دقت کرد که هرچه تعداد دستگاه هایی که به یک **UPS** وصل می شوند، بیشتر شود، میزان استفاده از باطری آن بیشتر و مدت زمان روشن نگه داشتن سخت افزارهای متصل شده، کمتر خواهد بود، به همین جهت، همیشه مهم ترین دستگاه ها، جهت اتصال به **UPS**، در اولویت تر هستند، ابتدا **Server** و سپس **Router**.

بطورمعمول پس از وصل کردن این کابل های موردنیاز، هم UPS و هم Server را روشن می کنیم و نرم افزار مربوط به UPS را بر روی Server نصب می کنیم و وارد تنظیمات آن می شویم.
بطور مثال می توان در بخش Email Setting مشخصات یک Email را وارد کرد، که در صورت بروز خطا یا خرابی در سیستم برق، یک ایمیل ارسال کند و ... .

نکته: UPS بهترین گزینه ی مقابله با خطرات و مشکلات ناشی از brownout می باشد.

نکته: UPS ها، دارای یک درگاه به نام درگاه Grounding هستند که اگر در مکانی که UPS را نصب می کنیم، سیم یا الکترود اتصال به زمین وجود داشته باشد، این درگاه را به آن متصل می کنیم.
اما این اتصال ارتباطی با کارآیی UPS ندارد و اجباری برای این اتصال وجود ندارد، اما انجام آن، از وقوع شوک های الکتریکی جلوگیری کرده و امکان برق گرفتگی در محیط را کاهش می دهد.

➢ :Power outage

اگر بدانیم که قرار است یک **Blackout** اتفاق بیفتد، اول از هرچیز خاموش کردن **Server** در اولویت اول قرار دارد.
به این صورت که به سادگی دکمه ی **Power** را یکبار کوتاه می فشاریم؛ و حدود **10** تا **15** دقیقه صبر می کنیم که بطورکامل خاموش شود.
پس دستگاه های دیگر، با قطع شدن برق، خودشان خاموش خواهند شد.

پس از اینکه جریان برق دوباره برقرار شد، **UPS** که خودش روشن می شود، اما به ترتیب زیر، دستگاه های دیگر را روشن می کنیم:

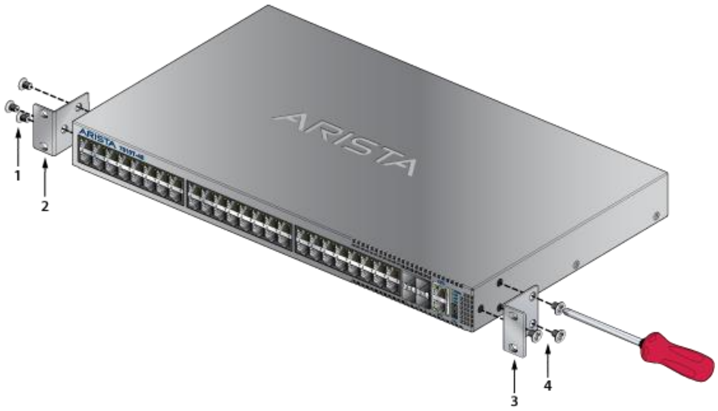
1. Router
2. Switch
3. Access Point

پس از حداقل **5** دقیقه

4. Server

: Rack

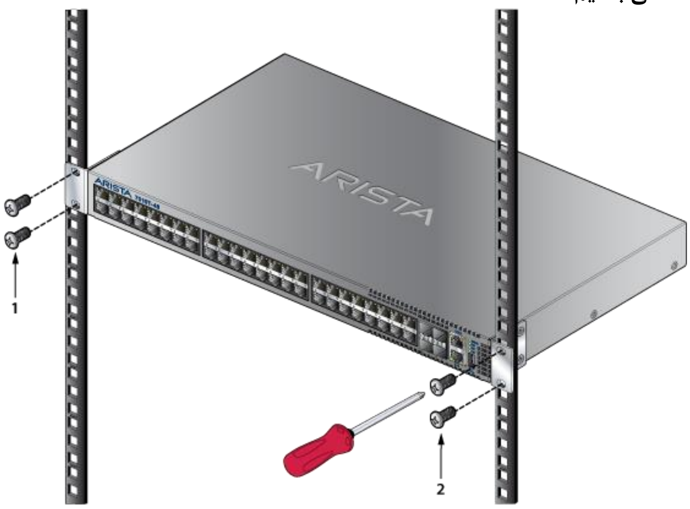
- محفظه ای که برای نگهداری متمرکز و امن دستگاه های شبکه استفاده می شود، **Rack** می باشد.
- به تجهیزی که قابل نصب در **Rack** باشد، **Rack mount** و یا **modular** گفته می شود.
- برای سوار کردن **Switch** یا **Router** بر روی **Rack**، از دو قطعه ی فلزی که همراه خود آنها در جعبه بوده است، که آنها را گوشواره یا **Mounting brackets** و یا (به آلمانی) **Ohren** می نامیم، استفاده می کنیم.
  - ابتدا یک سمت **Bracket** ها را در کناره های جلوی سوییچ می بندیم:



  - بر روی رک، در درگاه هایی که قصد داریم **Bracket** ها را به آنها ببندیم، نیاز به مهره ای داریم که روی بدنه ی **Rack** سوار می شود، بنام **Cage nut** و یا (به آلمانی) **Käfigmutter** که به شکل زیر آن را سوار می کنیم:



  - و سپس به شکل زیر، به سادگی، **Bracket** ها را به **Rack** می بندیم:

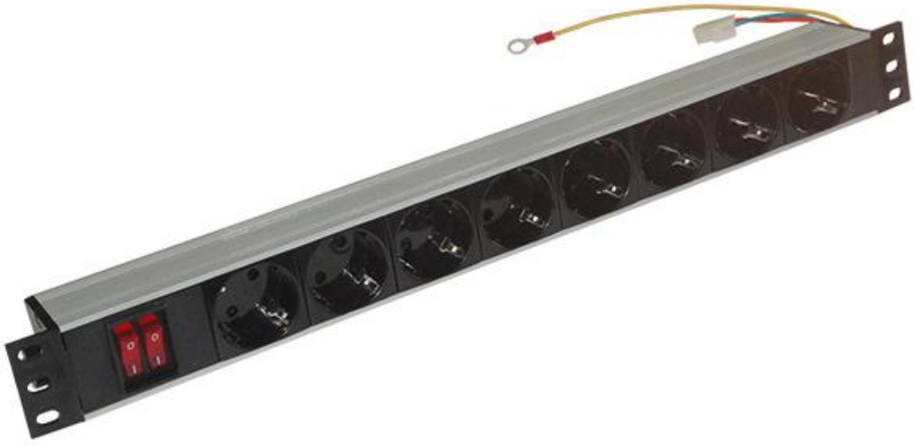


:Grounding system

Rack ها، دارای یک سیم به عنوان **Grounding** می باشند؛ جهت تخلیه ی الکتریسیته ی ساکن موجود و کاهش خطرات ناشی از آن.

:Power system

برای تامیین برق تجهیزات موجود در Rack، از یک Power module یا سیم سیار مخصوص Rack که تا مقدار آمپر بالا را پشتیبانی می کند، استفاده می کنیم. خیلی ضروری است که از یک power module قوی و متناسب استفاده شود.





:Fan system

برای جلوگیری از تجمع هوای گرم در درون فضای Rack، از قطعه ی تهویه ی هوا که معمولن همراه با خود Rack خریداری شده خواهد بود، استفاده می شود.



برخی Fan system ها، همچنین شامل یک حسگر دما هستند که براساس دمای موجود در Rack، بطورخودکار سرعت چرخش Fan ها را نیز تنظیم می کند.



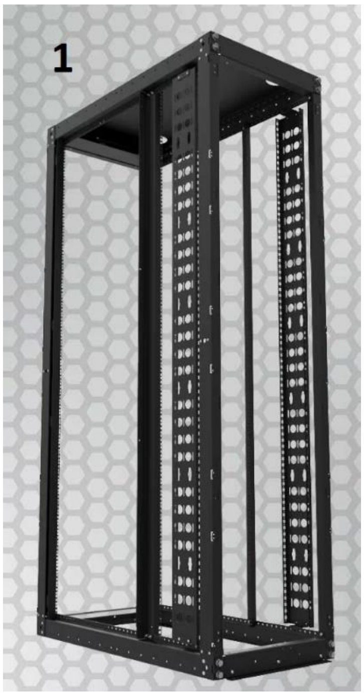
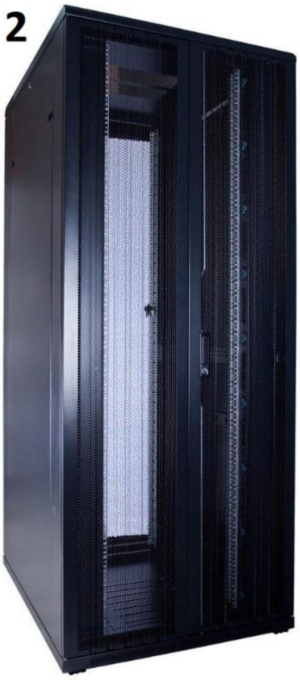
نکته: دمای معمول و مناسب برای همه تجهیزات موجود در Rack، بین 20 تا 24 درجه است.

:Rack Types ➢

بطورعمومی، چند نوع **Rack** وجود دارد:

1. **Open frame racks** (رک های باز):
2. **Enclosed racks** (رک های کمُدی):
3. **Wall-mounted racks** (رک های دیواری):
4. **Mobile racks** (رک های متحرک):
5. **Specialty racks** (رک های موارد خاص):

این نوع، برای نگهداری از تجهیزات خاص، مثل دستگاه های صوتی، تصویری و شبکه و ... استفاده می شود.

1

2

3

4

5


- **اگر تعداد تجهیزات شبکه، زیاد باشد، بسته به:**
  - **فضای امنیتی**
  - **شرایط آب و هوایی**
  - **تعداد دفعات موردنیاز به دسترسی به تجهیزات موجود در Rack، در بازه های زمانی کوتاه،**

  از یکی از گزینه های یک یا دو استفاده می کنیم.
- **همیشه برای وارد کردن و نصب دستگاه ها در Rack، پیشنهاد می شود که پایین به بالا، سوار و نصب کنیم.**

  بطورمثال، UPS که سنگین ترین دستگاه موجود در شبکه است، همیشه در پایین ترین فضای Rack نصب می شود.

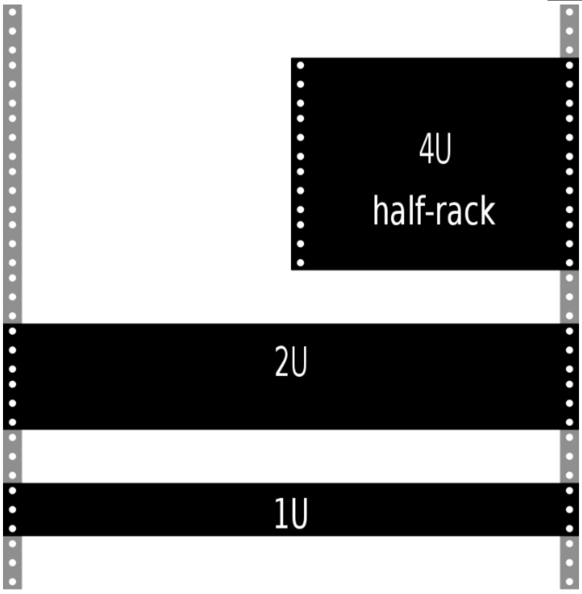
➢ :Rack heights

بسته به تعداد و نوع دستگاه هایی که قرار است در Rack سوار و نگهداری شوند، بطورطبیعی، ارتفاع Rack اهمیت خواهد داشت.

ارتفاع Rack ها را با واحدی به نام RU مشخص می کنند، که مخفف Rack Unit می باشد.

هر RU برابر است با: 1.75 inch یا 4.44 cm

اما به شکل ساده تر، هر سه سوراخ پشت سر هم بر روی بدنه ی Rack، برابر با یک Rack Unit می باشد.

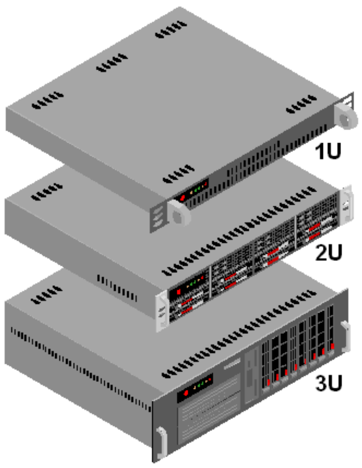


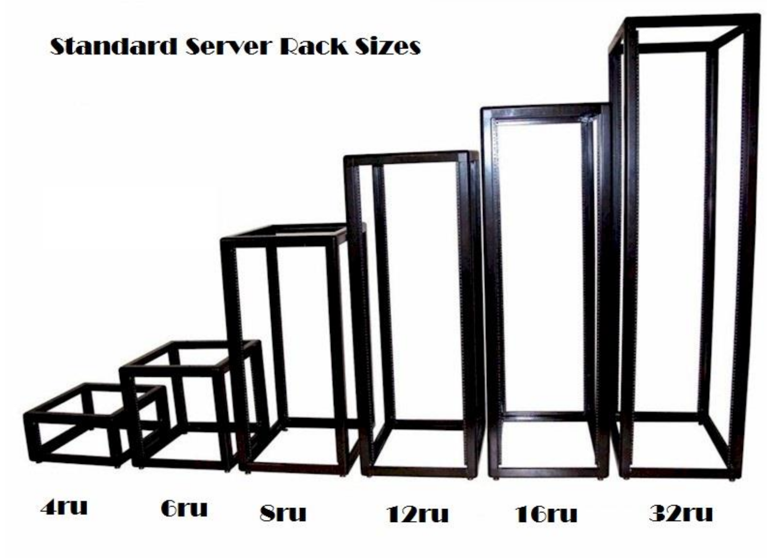
دلیل اینکه هر RU برابر با این مقدار است، این است که فضایی که بیشتر Switch ها و Router ها اشغال می کنند، برابر با مقدار 1 RU است.

پس اگر اندازه ی یک Rack برابر با 2 RU باشد، به این معناست که گنجایشی به اندازه ی دو دستگاه Switch یا Router را دارد.

از طرف دیگر:

- ✓ ابعاد دستگاه هایی مثل Server یا Storage ها، دوبرابر خواهد بود، یعنی هریک Server یا Storage ، به میزان حداقل 2 RU ارتفاع دارند.
- ✓ ابعاد Patch Panel ها، معمولن، نصف خواهد بود، یعنی هر Patch Panel ، نیاز به فضای 0.5 RU خواهد داشت.





بطور معمول:

- **رک های Wall-mounted، بین RU** 4 **تا RU** 8 **خواهند بود.**
- **رک های با ارتفاع RU** 12 **یا بالاتر، می توانند mobile Rack باشند.**
- **در صورت باقی ماندن فضای خالی در Rack، می توان از Blank Panel های یک، دو و یا چند Unit استفاده کرد، که ظاهر Rack، زننده نباشد.**

فرض کنید که:

- ✓ **یک Server با ارتفاع 2 RU،**
- ✓ **یک Switch با ارتفاع 1 RU،**
- ✓ **یک Firewall با ارتفاع 2 RU،**

در اختیار داریم.

پس به یک Rack احتیاج داریم که حداقل 5 RU ارتفاع داشته باشد.

درهنگام خرید یک Rack، باید به گزینه های زیر دقت کنیم:

- **وزن تک تک دستگاه هایی که باید در آن نصب شوند،**
- **عمقی که بزرگترین دستگاه از دستگاه های موردنظر دارد** (معمولن Server درازترین است، که نیاز به بیشترین عمق را خواهد داشت.)،
- **نوع قطعات جانبی که جهت نصب هریک از دستگاه ها در Rack، ضروری خواهند بود، مثل نوع mounting Rail ها که متفاوت هستند،**
- **قابلیت های مربوط به خود Rack؛** مثل mobile بودن، و یا درب داشتن و enclosed شدن.

:Patch Panel

برای اتصال کابلهایی که از سمت Client ها تا به سوی Rack کشیده شده اند و در Rack باید به Switch ها یا Router ها متصل شوند، از قطعه ای به نام Patch Panel و یا (به آلمانی) Patchfeld، استفاده می شود.

Patch Panel می‌بایست متناسب با کابل به کار رفته در سیستم انتخاب شود. به عنوان مثال اگر کابلی که از Client ها آمده است، Cat6 است، حتما باید پچ‌پنل و کابل‌های رابطِ Cat6 را تهیه کنیم. در صورت عدم سازگازی، سیگنالِ منتقل شده، ضعیف خواهد بود.

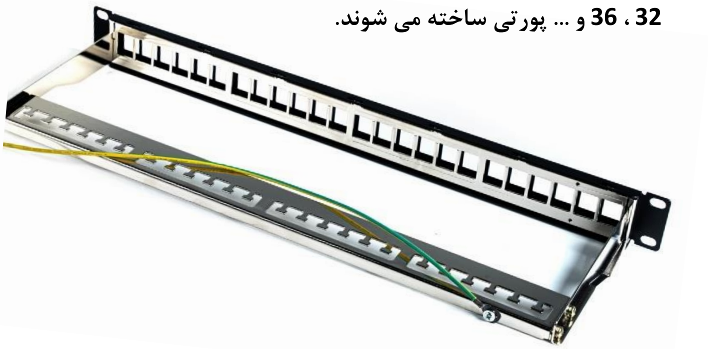
انواع Patch panel :

modular و یا unloaded:

در پچ پنل های ماژولار می توان چندین نوع پورت مثلاً UTP، STP و Cat5 , Cat5e , Cat6 , Cat7 و حتی انواع پورت فیبر نوری multi mode و single mode را در کنار هم قرار داد.

اگر پورتی به هر دلیلی دچار مشکل شود فقط همان پورت را تعویض می کنیم و نیاز به تعویض کامل پچ پنل نیست. این پچ پنل ها در انواع 12 ، 16 ، 24 ، 32 ، 36 و ... پورتی ساخته می شوند.





non-modular و یا loaded :

پچ پنل های غیر ماژولار در انواع Cat5e و Cat6 و Fiber optic و با تعداد پورتهای 16 ، 24 ، 36 و 48 پورت بصورت رنگی و مشکی تولید می شوند.

بطور معمول، عرض آنها 19 اینچ (حدود 48 سانتی متر) می باشد، و با همین عرض، Patch panel هایی با تعداد پورتهای مختلف تولید می شود.

مثلن نمونه های زیر همگی 19 اینچ هستند، با تعداد پورت های مختلف:





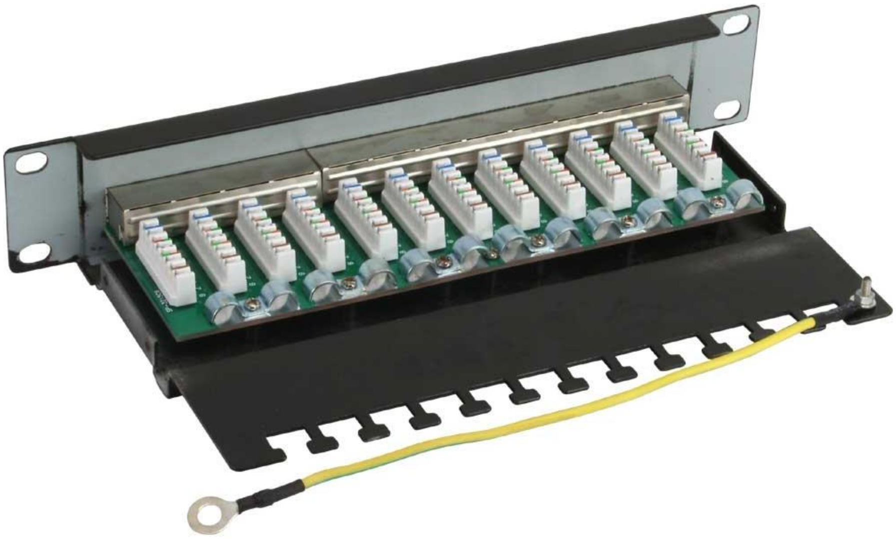


نکته: باید دقت کرد که Patch panel های Fiber optic، متفاوت از Patch panel های Twisted Pair خواهند بود.

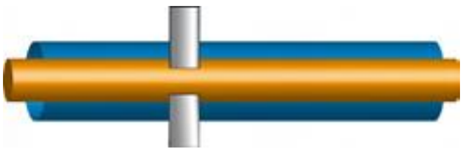
نکته: کابل کوتاهی که یک پورت از Patch Panel را به یک پورت از Switch وصل می کند، **Patch cord** نامیده می شود.



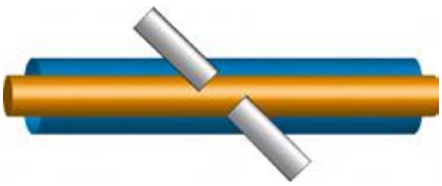
در شکل زیر، پشت یک Patch Panel مخصوص کابل های Twitsted Pair و non-modular را می بینیم، یعنی کابل های از سمت Client ها در Rack رسیده، یکی یکی به هر هشت شیار کنار هم، Punch می شوند:



اسلات LSA و +LSA: دو نوع Slot یا شیاری هستند که بر روی بورد های Patch panel های مخصوص کابل TP، برای هررشته سیم وجود دارند.



LSA



LSA+

رشته های سیم های کابل های TP را یکی یکی به روی شیارهای LSA یا +LSA پرِس و نصب می کنیم. این کار توسط ابزار Punch down Tool انجام می شود.



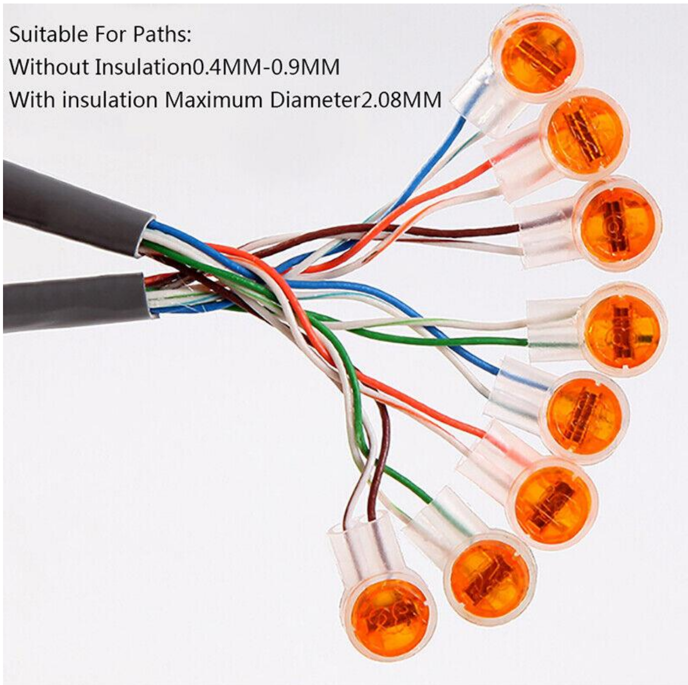
Gel Splice :

این قطعه، که به آن **Scotchlok** هم گفته می شود، جهت اتصال سر دو رشته سیم به یکدیگر بکار می رود، پس یک **Wire Terminal Connector** محسوب می شود.

به عبارتی، دو رشته سیم باریک را به هم متصل می کند.



بطورمثال، مطابق شکل زیر، می توان دو کابل **TP** را به یکدیگر پیوند زد:



Tape:

- ✓ به نگهداری **Backup** های یک شبکه، در جایی خارج از محل اصلی ذخیره سازی داده ها، off-site backup گفته می شود؛ که در صورت بروز هرگونه اتفاق و حادثه ی فاجعه بار، داده های پشتیبانگیری شده، همچنان صحیح و سالم باقی خواهند ماند.
- ✓ بطورکلی، به بازگردانی داده ها پس از وقوع یک حادثه ی ناگوار برای شبکه، Disaster Recovery گفته می شود.

- ✓ اهمیت اصلی **Tape** به عنوان رسانه ی پشتیبان گیری، قابلیت استفاده از آن به شکل off-site backup می باشد؛ که در صورت نیاز، به خوبی جهت **DR** (Disaster Recovery) مفید واقع می شوند.

- هرچند که سرعت **Restore** از روی **Tape**، پایین تر از **Restore** از روی دیسک هاست، اما مزیت **Tape** این است که **offline** کار کرده و داده های روی **Tape** ها، از **Virus** ها در امان خواهند بود.
- سرعت **Restore** داده از روی **Cloud** از سرعت **Restore** از روی **Tape** هم پایین تر است!
- سرعت انتقال داده های حجیم از شبکه به **Cloud** از سرعت انتقال از **Tape** به **Cloud** پایین تر است!
- **Tape** ها تا ظرفیت های **TeraByte** و **Peta Byte** و ... را نیز پشتیبانی می کنند.
- **Error Rates** در نوارها پایین است.
- طول عمر **Tape** ها بالاست، پس می توان به مدت طولانی، داده ها را درون آنها بایگانی کرد.
- به سادگی قابل حمل هستند.
- مصرف برق پایینی دارند.
- **Tape** دارای دسترسی خطی (Linear access) است، یعنی از آنجایی که **Tape** داده ها را به صورت **Serial** ذخیره می کند، برای اینکه مثلاً بخواهیم داده ای در انتهای نوار را بخوانیم، مجبور خواهیم بود کل نوار را طی کنیم! در حالی که **Cloud** ها دارای دسترسی **Random** هستند و قیمت تهیه ی **Cloud** از **Tape** هم کمتر خواهد بود.

- **Tape Drive:**
  - یک **Tape Reader Drive** است که توسط جریان مغناطیسی ای که دارد، اطلاعات را روی نوار نوشته یا از روی آن می خواند.
  - کاملاً مشابه با دستگاه های پخش **Video** قدیمی است، که ابعاد کوچکتری دارد.
  - می تواند مستقیم به **Server** متصل شود.
  - درهرلحظه فقط می تواند یا اطلاعات را بنویسد یا فقط بخواند، اما هردو را بطورهمزمان نمی تواند.
- **Tape Cartridge:**
  - دارای یک **magnetic tape** بلند و باریک است.
  - کاملاً مشابه با همان **Video cassette tape** و **Audio cassette tape** می باشد، اما با ظرفیت خیلی بیشتر.
  - توسط جریان مغناطیسی که در **Tape Drive** وجود دارد، اطلاعات روی **magnetic tape** نوشته یا از روی آن خوانده می شوند.
  - **از نسل سوم به بعد**، تکنولوژی **WORM** (**Write Once Read Many**) اضافه شد تا از قابلیت **Rewritable** یا **overwriting** (بر اثر خطای انسانی) جلوگیری کند.
  - **از نسل چهارم به بعد**، قابلیت **Encryption** اضافه شد، که می تواند بعد از **Compression** انجام شود.
  - از نسل پنجم به بعد، قابلیت **Partitioning** اضافه شد که کنترل و مدیریت فضای را بهبود بخشید.
  - آخرین نسل آنها، **LTO** (**Linear Tape-Open**) است، که تا نسخه ی **LTO8** آمده است که قادر به استفاده در کنار دستگاه های تا دو نسل قبل از خودش نیز می باشد، و به صورت معمول تا **9TB**، و به صورت فشرده تا **22.5TB** قادر به ذخیره سازی است.
  - میزان **BER** (**Bit Rate Error**) در نوارهای **LTO7** و **LTO8** به مقدار 10^{-19} رسیده است، که چهار برابر بهتر از **HDD** است.
  - **LTO1** سال **2000** معرفی شد.

- **:Tape Autoloader**
  - شامل یک **Tape Drive** و چند **Tape Cartridge** و یک بازوی خودکار جهت تعویض و جابجایی **Tape** ها می باشد.
  - مدیریت از راه دور آن (**Remote Management**) بر پایه ی **web** می باشد.
  - مخصوص **SMB** هاست.
- **:Tape Library**
  - یک دستگاه با ابعاد بزرگتر است که شامل چندین **Tape Drive** و چندین **Tape Cartridge** می باشد.
  - به نوعی، یک ترکیب بزرگ از چند **Tape Autoloader** با همدیگر است.

➢ RDX (Removable Disk Storage):

این نوع نوارهای مغناطیسی، مزایای دیسک های سخت و درایوهای نوار مغناطیسی معمولی (LTO) را با هم دارند.
سرعت بالایی در دستیابی به اطلاعات و انتقال آنها دارند.
RDX شامل یک دیسک خوان است که نوار یا دیسکِ آن، همراهش است.

: Work Group/Domain Network

در حقیقت، در شبکه های **Work Group**، اعضای شبکه، تعدادی سخت افزار شامل **PC** ، **Mobile** ، **Labtop** و ... هستند که هرکدام از **PC** ها دارای یک یا چند حساب کاربری بر روی خودشان هستند و آنها را روی خودشان تنظیم می کنیم.

اما در شبکه های **Domain**، اعضای شبکه، تعدادی حساب نرم افزاری یا **Account** هستند که از هر سخت افزار متصل به شبکه، می توان با وارد کردن مشخصات (نام و پسورد) یکی از **Account** ها، وارد محیط شبکه شد.
این حساب های کاربری، در سیستم **Server**، که مدیریت شبکه را به عهده دارد، تنظیم می شوند.
سیستم **Server**، سیستم عامل **Server** دارد.

از ویژگی های شبکه **Domain**:

- هم برای شبکه های کوچک و هم برای شبکه های بزرگ می توان از آن استفاده کرد.
- این نوع شبکه دارای یک مدیر است که سیستم **Server** را کنترل می کند.
- سیستم های دیگر، **Client** نام دارند که دارای سیستم عامل های معمولی خواهند بود.
- برای اینکه سیستم عامل **Server** بتواند از قابلیت های مدیریتی اش استفاده کند، هریک از بخش های مدیریتی اش را در قالب یک **Service** نصب کرده و استفاده می کنیم.
- سرویس های مهم آن **Active Directory** ، **DHCP** و **DNS** هستند.
- **Data Base** مرکزی آن، در سرویس **Active Directory** قرار دارد.
- کامپیوترها بصورت **Automatic** از سرویس **DHCP**، **IP** دریافت می کنند.
- **Admin** شبکه می تواند کاربرانی را در سطح دسترسی و مدیریت خودش نیز تعریف کند.

پس وقتی دستگاهی، به یک شبکه وارد می شود، دو حالت دارد:

- اگر مدیریت شبکه از نوع **Work group** باشد، دستگاهِ جدید، هم-سطح با اعضای قدیمی، در شبکه حضور خواهد داشت.
- اگر مدیریت شبکه از نوع **Domain** باشد، دستگاه جدید، طبق **Authorization** ای که از طرف **Admin** برایش تعریف می شود، دارای حقوق و سطح دسترسی مشخصی خواهد بود.

Authorization و یا کنترل سطح دسترسی، مشخص می کند که یک کاربرِ مجاز (تشخیص هویت داده شده یا Authenticated User) چه کار می تواند بکند و به چه اطلاعاتی می تواند دسترسی داشته باشد.

در شبکه ی **Work Group**، برای **Account** های تعریف شده ی هر سیستم:

- اطلاعات مربوط به **Athentication** یا احراز هویت (Username و Password)
- اطلاعات مربوط به **Authorization** یا کنترل دسترسی (Access level)

در یک فایل **Data Base** به نام **SAM** (Security Account Manager) درخود هر سیستم (local) ذخیره می شوند.
فایل **SAM** در سیستم در مسیر C:\Windows\System32\config\SAM قرار دارد.

در شبکه های **Domain**، فایلی به نام **SAM** وجود ندارد، چون اطلاعات مربوط به همه ی **Account** ها، در سیستم **Server** و در کنسول **Active Directory** ذخیره می شوند.

Port:

در حقیقت Port ها، درگاه های منطقی (نرم افزاری) برای مبادله ی اطلاعات هستند، که هریک از آنها را با یک شماره، مشخص می کنیم.
Port ها، چیزی جز شماره نیستند. شماره هایی جهت آدرس دهی در لایه ی Transport.

- Port Number (که معمولا یک عدد ۱۶ بیتی است) برای تعیین اینکه یک بسته اطلاعاتی (packet) در اینترنت یا سایر شبکه‌ها، دقیقاً به چه برنامه ای در رایانه ی مقصد تعلق دارد، استفاده می شود.
- در حقیقت هریک از سرویس های سیستم، از یک Port معروف استفاده می کنند.
- نکته اینجاست که همانطور که می دانیم ارسال و دریافت data در شبکه به دو شکل Packet و یا Datagram انجام می شود.
- TCP به صورت Packet کار می کند.
- UDP به صورت Datagram کار می کند.
- هر سرویس می تواند با هریک از پروتکل های TCP و UDP بطورجداگانه کار کند.
- هر Packet ای که در شبکه ارسال یا دریافت می شود، دارای دو Port Number است:
  - Source Port: عددی 16 بیتی است که شماره پورتی که در فرستنده، از آن ارسال شده است را نشان می دهد.
  - Destination Port: عددی 16 بیتی است که شماره پورتی که در گیرنده، به آن وارد خواهد شد را نشان می دهد.

  بطورمعمول، این دو شماره برای یک Packet یکسان هستند، مگر در موارد خاص!

پس وقتی می گوییم شماره ی Port یک سرویس، فلان عدد است، یعنی این سرویس هم برای پروتکل TCP و هم برای پروتکل UDP با این شماره پورت کار می کند. اما باید بدانیم که توسط هریک از این پروتکل ها، چه کاری انجام می دهد!

- مثلاً شماره پورت سرویس DNS، عدد 53 است.

مطمئناً کاری که سرویس DNS توسط پروتکل های TCP و UDP انجام می دهد، در یک زمینه ی کاری هستند، اما در نهایت کاملاً یکسان نیستند و به منظورهای متفاوتی هستند.

در پروتکل های ارتباطی TCP وUDP ، این عدد ۱۶ بیتی در header مربوط به بسته قرار گرفته و ارسال می شود.
اگر یک Packet فاقد Port Number باشد، سیستمی که Packet را دریافت می کند، نمی داند که آن را باید به کدام نرم افزار ارسال کند.

شماره ی IP Destination موجود در بسته ی ارسالی، به Router ها و Switch های شبکه می گوید که این بسته به کدام بخش شبکه و کدام کامپیوتر شبکه باید برود، و وقتی که بسته به کامپیوتر مقصد رسید، Port Number موجود در آن، به کامپیوتر مقصد می گوید که به کدام بخش نرم افزاری روی آن باید برود.

مثال: وقتی به یک Website وصل می‌شویم و یک Web page را درخواست می‌کنیم، مرورگر به پورت ۸۰ کامپیوتر مقصد وصل می‌شود.
مثال: فرض کنید درخواستی از کامپیوتر خود به سرور، برای دریافت یک فایل از طریق FTP ارسال می کنید.
در این حالت پروتکل TCP کامپیوتر شما برای ارسال این درخواست به پروتکل FTP سرور مقصد، در Header بسته ی ارسالی خود، شماره ی پورت 21 (که پورت مخصوص FTP می باشد) را می گنجاند.
و این Packet از طریق پروتکل TCP در Server مقصد خوانده شده و با توجه به شماره پورت 21، به برنامه ی FTP جهت پردازش های بعدی ارسال می شود.
پس در حقیقت به این شکل است که برای برخی از برنامه ها و پردازش ها، به شکل قراردادی اعداد ثابتی به عنوان پورت اختصاصی آنها درنظر گرفته شده است.

- گاهی برای برقراری ارتباط توسط یک IP در بستر یک Port خاص، آنها را بصورت زیر درج می کنند، که به این حالت نوشتاری Socket گفته می شود (مثلاً ارتباط توسط FTP):

192.168.139.1:21

➢ Port Number Types:

1. Well Known Port Numbers :

- شماره پورت هایی هستند که شناخته شده یا مشهور هستند و برای Application های رایج استفاده می شوند.
- محدوده ی این Port Number ها از 1 تا 1023 می باشد.
- مثلاً شماره پورتِ web، که برابر با عدد 80 است، و پورت های HTTP، HTTPS، FTP، DNS و ....
- برای مشاهده ی Port Number های well known می توان به آدرس زیر مراجعه کرد:

www.tcp-udp-ports.com/ports0-1000.htm

Port Number	Protocol	Application
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL

7	TCP/UDP
443	https
3389	(RDP) Remote Desktop Connection
20 و 21	FTP
22	SSH
143	IMAP4
53	DNS

2. Registered Port Numbers :

- شماره پورت هایی هستند که شرکتها از آنها در Application هایی که خیلی رایج نیستند، استفاده می کنند.
- محدوده ی این Port Number ها از 1024 تا 49151 می باشد.

3. Dynamic/Random Port Numbers :

- شامل شماره پورت هایی است که به صورت تصادفی به End User یا کاربران اختصاص داده می شوند و هیچگاه برای یک کاربر یکسان نخواهد بود و هر بار اعداد آنها با یکدیگر متفاوت خواهند بود.
- محدوده ی این Port Number ها از 49152 تا 65535 می باشد.

File Transfer :

دستگاه های متصل به شبکه، به روش های متفاوتی اقدام به انتقال فایل می کنند، که به نوع آن دستگاه و نوع سیستم عامل ها بستگی دارد.

➢ FTP (File Transfer Protocol):

این یک روش استاندارد برای جابجایی فایل‌ها بین یک Client و یک Server است.
نوع سیستم عامل مورد استفاده ی شما برای FTP مهم نیست.
این پروتکل از سال‌های دور و پیش از آن که هیچ نوع رابط گرافیکی داشته باشد، مطرح بوده است.

شماره پورت مورداستفاده برای این پروتکل، 21 می باشد.

حتی ممکن است یک Router مجهز به یک درگاه USB باشد که امکان انتقال فایل به یک درایو external را از طریق FTP فراهم سازد. اما به اندازه ی راه‌اندازی یک رایانه اختصاصی برای این کار (File Server) پایدار نیست.
هنگام استفاده از FTP می‌توانید با تعیین یک نام کاربری و رمز عبور از داده‌های خود حفاظت کنید.
اما FTP به صورت پیش‌فرض، این اطلاعات authenticate را بدون رمزنگاری انتقال می‌دهد. این کار در شبکه ی خانگی ممکن است عیبی نداشته باشد، اما زمانی که در یک شبکه ی بزرگ‌تر مثل اینترنت کار می‌کنیم، به روش مطمئن‌تری نیاز داریم.
البته این به آن معنی نیست که باید FTP را کنار بگذاریم. می‌توان از FTPS استفاده کرد که نسخه‌ای از FTP است که اتصال‌ها را رمزنگاری می‌کند.

➢ SMB (Server Message Block):

زمانی که یک فایل را ایجاد کرده و با استفاده از File Explorer ویندوز، به کاربران دیگر در سطح LAN دسترسی می‌دهید، در واقع از SMB استفاده می‌کنید.
البته امکان دسترسی به این فایل‌های اشتراک گذاری شده برای کاربران Linux و macOS نیز وجود دارد.
نسخه ی SMB برای سیستم های macOS را، SMBX نامگذاری کرده اند.
نسخه ی SMB برای سیستم های Linux را، Samba نامگذاری کرده اند.

شماره پورت مورداستفاده برای این پروتکل، 445 می باشد.

Data transmission Mediums:

در یک شبکه، برای ارسال و دریافت اطلاعات از **Source** تا **Destination**، با دو نوع کلی کانال، روبرو هستیم:

- **Wired** یا **Cables** که به آنها **Guided** (هدایت شده) هم گفته می شود.
  - Coaxial
  - Twisted Pair
  - Fiber Optic

- **Wireless** که به آنها **Unguided** (هدایت نشده) هم گفته می شود:
  - **IR** (Infrared Radiation):

    همانطور که می دانیم، رنگ قرمز، طولانی ترین طول موج را دارد، به همین دلیل در شب، رنگ قرمز راحت تر و از دورترین فاصله ها دیده می شود.

    اما موج فروسرخ، یک تابش الکترومغناطیسی است که طول موج آن بیشتر از امواج مرئی (که آخرین موج مرئی، قرمزرنگ است) و کمتر از امواج رادیویی است.

    یعنی نه با چشم دیده می شود، و نه روی امواج رادیویی تاثیری می گذارد.
  - **RF** (Radio Frequency)
  - **NFC** (Near-Field Communication)
  - **Bluetooth**

: USB Cables

بطور معمول کابل **USB** ، کابلی **passive** است، که یک سرش نر (male plug) و سر دیگرش مادگی (Socket) است، اما گاهی در بین مسیرش از یک **booster** (تقویت کننده) **5** ولتی برای تقویت استفاده می شود که در این حالت آنرا **Active** گویند.

- اگر هردو سر نری و مادگی کابل **USB** از یک نوع باشند، یعنی **AA** یا **BB** ؛ آنوقت آنرا **USB Extender** یا **USB Verlängerung** گویند.
- اگر **USB Extender** بدون کابل باشد، آنرا **USB Adapter** گویند. (تبدیل)
- اگر هر دو طرف **Extender** از نوع **Socket** (مادگی) باشند، آنرا **Verbinder** یا **Connector** گویند.

حداکثر طول کابل **USB** :

- **USB 2 Passive** : 5 متر
- **USB 2 Active** : 20 متر
- **USB 3 Passive** : 3 متر
- **USB 3 Active** : 10 متر

برای استفاده از **USB HUB** حداکثر از **5** هاب برای طول **30** متر می‌توان استفاده کرد.

:Video Cables

کابل VGA و کابل های Composite تنها قادر به انتقال سیگنال‌های ویدئویی آنالوگ هستند. این کابل‌ها برای نمایشگرهای CRT بهترین گزینه بودند و هستند ولی برای LCD ها گزینه ی مناسبی نیستند.
حداکثر طول کابل VGA به شرط عدم افت کیفیت، 10 متر است.

DVI (Digital Visual Interface) :

- **قابلیت انتقال صوت را ندارد.**
- **حداکثر دارای 24 پین است، که اگر تعداد پین ها کمتر باشند، فقط قابلیت پشتیبانی تا کیفیت های پایین تری را دارد.**
- **از سیگنال‌های آنالوگ نیز همانند دیجیتال پشتیبانی به عمل می‌آورند.**
- **حداکثر طول آن 10 متر است.**

HDMI :

- **می توانند صدا و تصویر را به صورت همزمان انتقال دهند.**
- **حداکثر طول آن 20 متر است اما نوعی از این کابل تولید می شود که دارای چیپ تقویت کننده ی داخلی می باشد، که از 5 ولت سیگنال که برای انتقال داده استفاده می شود، بهره می برد، به همین سبب تا طول 40 متر هم می تواند برسد.**

DisplayPort :

- **می توانند صدا و تصویر را به صورت همزمان انتقال دهند.**
- **حداکثر طول آن 5 متر است.**

مقایسه ی کیفیت ارسال تصویر در کابل های ویدیویی:

VGA < HDMI < DVI < DisplayPort

نکته: به ترانس یا booster های روی کابل های انتقال تصویر، Ferrite یا Ferrite Core گفته می شود که باعث کاهش نویز و پایداری کیفیت سیگنال می شوند.

: Coaxial Cables

بطورکلی به دو دسته تقسیم می شوند:

- **Thin net:** حداکثر طول: 185 m
  استاندارد کارآیی این کابل، 10base2 است، چراکه سرعت 10Mb/s را تا 200 متر پشتیبانی می کند.
  مدل کابلی که این حالت را پشتیبانی می کند، RG-59 می باشد.

- **Thick net:** حداکثر طول: 500 m
  استاندارد کارآیی این کابل، 10base5 است، چراکه سرعت 10Mb/s را تا 500 متر پشتیبانی می کند.
  مدل کابلی که این حالت را پشتیبانی می کند، RG-58 می باشد.

از لحاظ قدرت بکارگیری، به چند دسته تقسیم می شود که نام آنها با RG (Radio Guide) شروع می شوند.
اما دو دسته ی پر کاربرد کابل های Coaxial که دارای قدرت و پهنای باندهای متفاوت هستند: RG-59 و RG-11
در تصویر زیر مثال خوبی برای مقایسه ی برخی از کابل های کواکسیال است:



RG-6 کابل انتخابی برای گیرنده های ماهواره ای است، زیرا کیفیت سیگنال بهتری دارد.
RG59 برای سیگنال های ویدئویی استفاده می شود، زیرا کیفیت خیلی مناسبی خواهد داشت.

- سوکت یا Connector مورداستفاده، جهت اتصال کابل های کواکسیال، BNC نام دارد.

اصطلاحات:

Cross Talk : تأثیر منفی سیگنالهای الکتریکی دو کابل بر یکدیگر

Attenuation (تضعیف): کاهش توانایی سیگنال عبوری از کابل، به دلیل افزایش فاصله فرستنده و گیرنده.

Twisted Pair Cable :

کابل های Twisted Pair که جهت ارتباط کابلی شبکه استفاده می شوند، بطورکلی به دو دسته تقسیم می شوند:
- UTP (Unshielded Twisted Pair)
- STP (Shielded Twisted Pair)

- کابل شبکه، Ethernet Cable یا LAN Cable هم نامیده می شود.
- کابل شبکه مثل کابل تلفن است اما کابل تلفن از 2 یا 4 رشته استفاده می کند، کابل شبکه از 8 رشته.
- البته لزومی به 8 عدد سیم هم نیست، چون انتقال تا پهنای باند 100 مگابیت برثانیه را می شود با چهارسیم(two Twisted Pair) انجام داد. دو سیم برای send و دو سیم برای Receive داده ها.
- زوج سیمِ ارسال را با TX و زوج سیمِ دریافت را با RX نشان می دهند.
- دلیل اینکه از زوج سیم استفاده می شود این است که هر سیگنال یک بخش مثبت و یک بخش منفی دارد.

در نتیجه یک RX+ و یک RX− و همچنین یک TX+ و یک TX− وجود خواهد داشت.
- اما در GigaBit Networks، سرعت انتقال به 1000 مگابیت بر ثانیه می رسد که، از 4 سیم برای انتقال و از 4 سیم برای دریافت Data استفاده می شود.
- Connector این کابل، RJ45 است که برای شبکه های Ethernet و همچنین Token Ring استفاده می شود.

نسل کابل های Twisted Pair :
- Category 7A : پهنای باند 1000 MHz و سرعت 10000 MbpS (10 GbpS)
- Category 7 : پهنای باند 600 MHz و سرعت 10000 MbpS (10 GbpS)
- Category 6A : پهنای باند 500 MHz و سرعت 10000 MbpS (10 GbpS)
- Category 6 : پهنای باند 250 MHz و سرعت 1000 MbpS (1 GbpS)
- Category 5e : پهنای باند 100 MHz و سرعت 1000 MbpS (1 GbpS)
- Category 5 : تا سرعت 100 MbpS قابل بکارگیری است.

❖ پسوند A که بعد از نام برخی دسته بندی های کابل وجود دارد، اختصاری برای Augmented به معنی افزوده شده یا تکمیل شده است.
❖ حداکثر طول کابل های زوج سیم، 100 متر می تواند باشد.
❖ data transfer Speed در کامپیوتر ها و Switch های معمولی، برابر است با 1 Gb/Sec .

نکته: تفاوت مهم نسل های مختلف کابل ها این است که در هر نسل، سرعت انتقال افزایش و میزان نویز کاهش پیدا می کند، که این عمل به دو طریق انجام می شود:
- روکش گذاری (shield)
- پیچش بیشتر زوج سیم ها به هم

Connector یا سوکت قابل استفاده برای کابلهای زوج سیم بهم تابیده، RJ-45 می باشد؛ که برای اتصال آن به سر کابل، دو نوع استاندارد A و B وجود دارد. اگر سوکت های دوسر یک کابل را با استاندارد مشابه، پرس کنیم، به آن کابل Cross گفته می شود و اگر نامشابه پرس کنیم، به آن کابل Straight گفته می شود.
- Cross over برای اتصال دو دستگاه مشابه بکار می رود.
- Straight برای اتصال دو دستگاه غیرمشابه بکار می رود.

نکته: امروزه، مودم های کامپیوترها هوشمندتر شده اند، در نتیجه ی اینکه یک کابل Cross باشد یا straight، اهمیتی نخواهد داشت.

➢ Telefone Cables:

Connector یا plug قابل استفاده برای اتصال سیم تلفن به گوشی تلفن، RJ-11 می باشد.

به کابل تلفنی که دوسرش دارای سوکت پرس شده و آماده ی استفاده باشند، modular Cable گفته می شود.

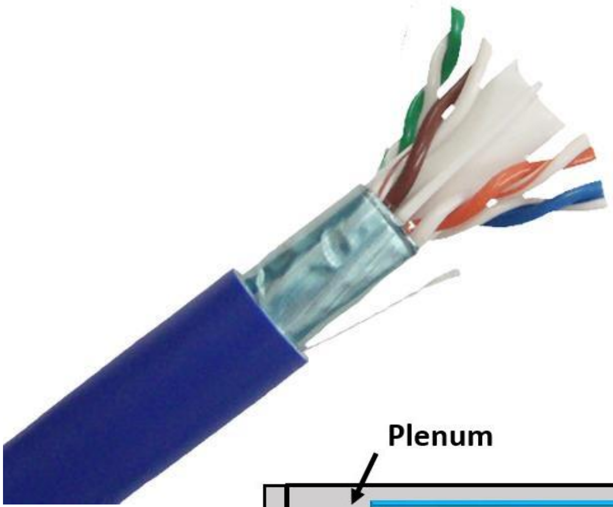
شرکت هایی وجود دارند که modular cable های با طول متفاوت، برای فروش ارایه می کنند.

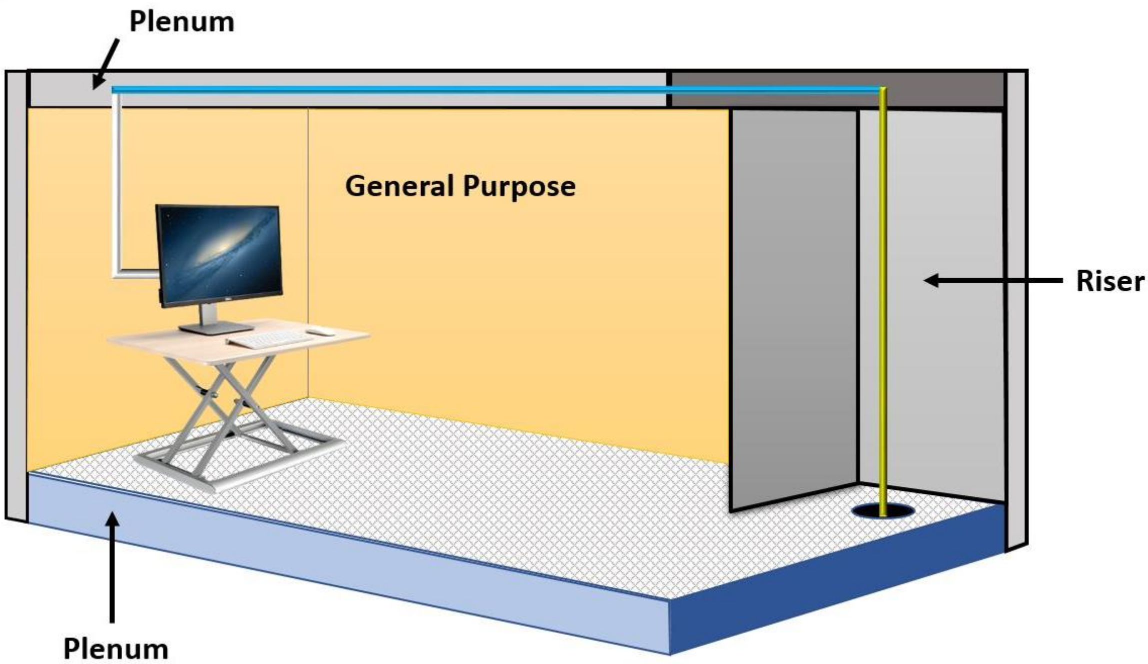
- **دو سر RJ-11**
- **یک سر RJ-11 و یک سر RJ-45**
- **دو سر RJ-45**

نکته: وقتی دو سر یک کابل، RJ-45 باشد، طوری که در هر طرف فقط چهار رشته از سیم ها پرس شده باشند، به عنوان کابل تلفن ISDN از آن استفاده می شود.

➢ Plenum Cables :

کابل TP ای است که ضد دود و آتش بوده و جهت استفاده در سقف ها یا کف های کاذب بکار می رود.

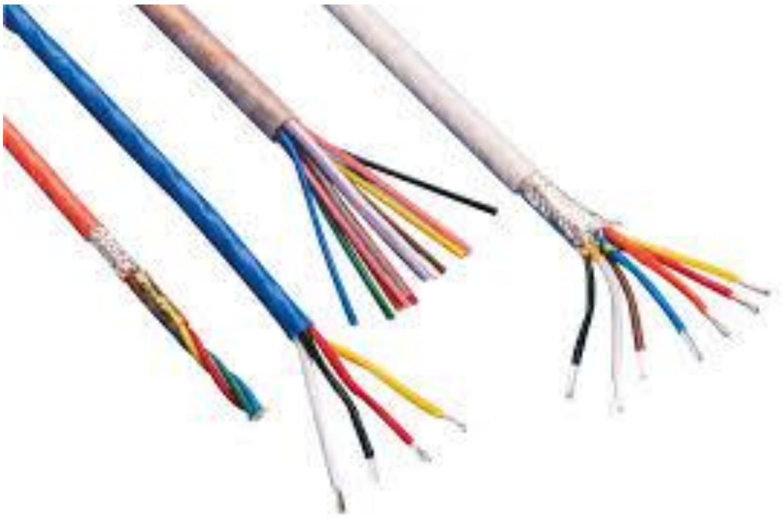




➢ Twisted Pair components :

- ❖ **plastic cover** : پوشش پلایتیکی ضخیم روی کابل است که برای برش دادن آن از **Stripper** استفاده می شود.
- ❖ **braid** : رشته سیم های ظریف به هم بافته شده ای که به عنوان نویزگیر استفاده می شوند.
- ❖ **Foil** و یا **Aluminum sheet** : ورق آلومینیومی ظریفی است که پیرامون همه ی سیم ها و یا زوج سیم ها را می پوشاند.

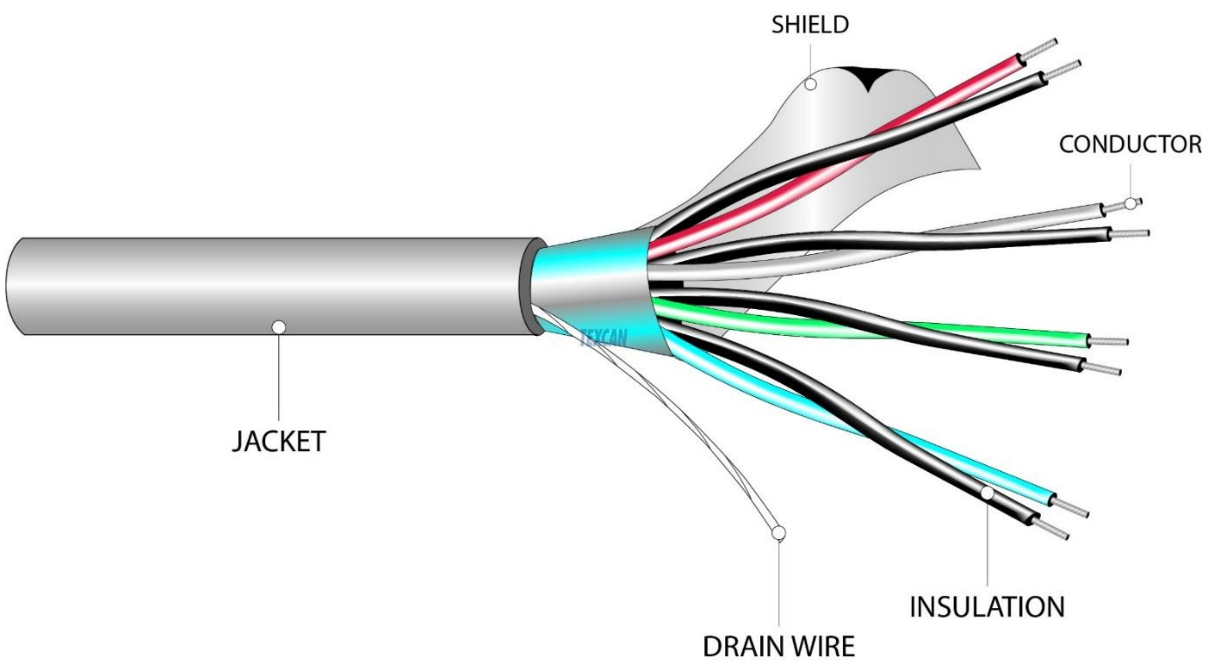
Litz wire یا **Litze**: مجموعه ای از رشته سیم های به هم پیچیده شده است که یا پوشش رنگی ظریف پلاستیکی دارند، و یا در کابل های برق، به شکل بدون عایق به هم پیچیده شده اند.



Strand : هر یک رشته ی **Litz**، یک **strand** است که شامل دو بخش است:

- ○ **PVC insulation**
- ○ **Conductor** (بخش مسی سیم)





Stranded Cable : کابلی است که فقط دارای **Litz** و حداکثر یک **braided shield** است. به همین جهت انعطاف بالایی داشته و برای ساخت **Patch cable** استفاده می شود.

Cabling Wire و یا Solid wire : کابلی ضخیمی است که شامل **Litz** ، **braided shield** و **Foil** می باشد.
از این کابل برای کابلکشی و انتقال اطلاعات در مسافت های بیشتر از دو سه متر استفاده می شود که در دو طرف آن، یک **Keystone** (مادگی **RJ-45**) نصب می شود.
در یک سمت، **Keystone** در پریز شبکه نصب می شود و در طرف دیگر، **Keystone** در **Patch panel** نصب می شود.



- یکی از قوانین مهم در شبکه این است که سرعتِ یک ارتباط، تابع سرعتِ سمت کُندتر است.

بطور مثال اگر در شبکه ای از کابل **CAT 6** استفاده شده باشد، هنوز هم می توان از **CAT 5** استفاده کرد، اما سرعت شبکه تحت تأثیر سرعت پایینِ کابل **CAT 5** قرار خواهد گرفت.

Fiber optic Cable :

Fiber دارای سرعتی حدود **10 Gbps** تا **100 Gbps** می باشد.

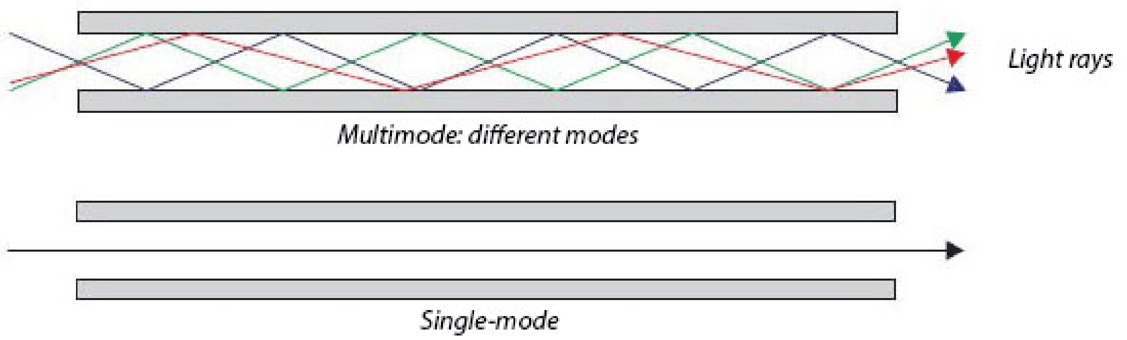
از مهم ترین مزایای کابل نوری این است که **Noise** و اختلالات الکترونیکی بر روی بستر انتقال آن، یعنی نور، تأثیری ندارند.

انواع فیبرنوری از لحاظ میزان انتقال داده:

- **Single Mode Fiber** (SMF): کابلی با دوام بالاست که می تواند انتقال در فواصل طولانی (تا 80 کیلومتر) را پشتیبانی کند، اما فقط قادر به ارسال یک سیگنال در زمان است. از **Laser** برای تولید نور استفاده می کند. قطر هسته ی آن بین **5** تا **9** میکرومتر است.

  کابل‌های **Single mode** به دو دسته ی **OS1** و **OS2** تقسیم می‌شوند.
  تفاوت آن‌ها در طول موج و نحوه ی انتشار نور در هسته می‌باشد.

- **Multi Mode Fiber** (MMF): قادر به ارسال چند سیگنال بطور همزمان است. برای انتقال همزمان انواع فایل در فواصل کوتاه تر (تا 500 متر) کاربرد دارد. چون هسته یا هسته های این فیبر طوری هستند که می توان چند سیگنال با زوایای تابش مختلف را ارسال کرد. از **LED** برای تولید نور در آن استفاده می شود.
  - هرقدر قطر هسته ی آن کمتر باشد، کیفیت سیگنال را برای مسافت های طولانی تری حفظ خواهد کرد، و بالعکس.

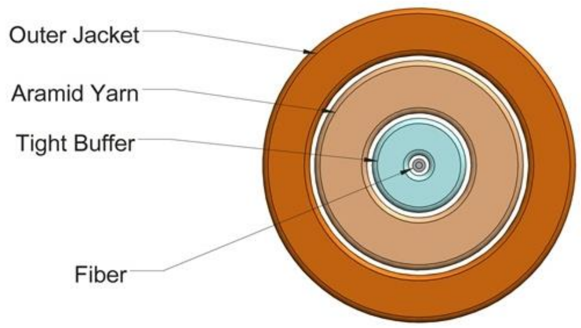


انواع فیبرهای **Multimode** (Optical Multimode) :

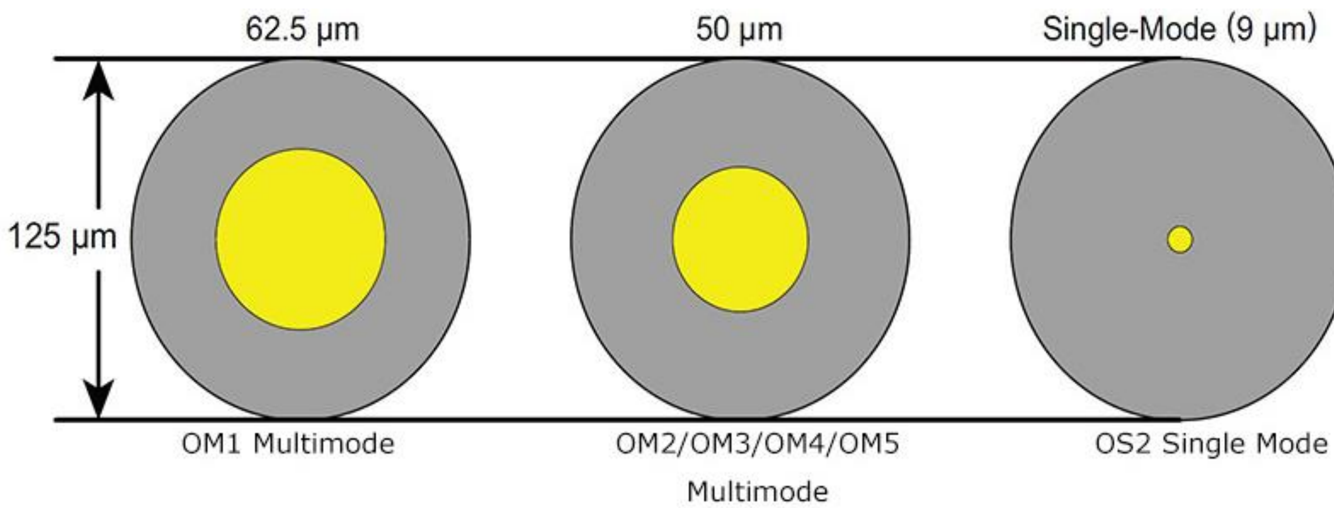
- **OM1** :

به طور معمول دارای یک **Jacket** یا روکش نارنجی و **Core** با قطر **62.5** میکرومتر (µm) است.

این کابل می تواند **10 Gbps** در طول **33** متر را پشتیبانی کند.







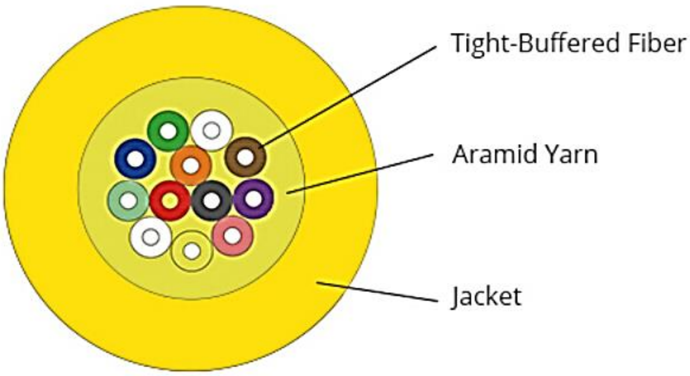
انواع فیبرنوری از لحاظ مکان و فضای انتقال:

❖ **Indoor : برای کابل کشی در محیط های بسته و داخل ساختمانی بکار می رود. Jacket آن PVC است.**
پوشش روی این کابل، Tight Buffer است.

➢ **Tight Buffer** روکش پلاستیکی است که هسته ی فیبر را می پوشاند و قطر آن 900 میکرومتر است که از ضربه‌های کوچک به فیبر جلوگیری می‌کند.

➢ **Aramid Yarn** : مجموعه ای از رشته نخ‌هایی ست که بر روی Tight Buffer قرار می گیرند. این پوشش موجب منعطف‌تر شدن کابل شده و استفاده از آن را برای کاربردهای متنوع آسان‌تر می‌کند.





دو نوع Aramid Yarn وجود دارد:

1. **Breakout : در این نوع کابل، برای هر هسته ی فیبر، یک پوشش وجود دارد.**
2. **Mini-Breakout : در این نوع کابل، یک پوشش واحد، کل فیبرها را حفاظت می کند.**





❖ **Outdoor** : برای کابل کشی در محیطهای پیچیده ی بیرون ساختمانی بکار می رود. **Jacket** آن **PE** (Polyethylene) است.

✓ به کابل های **Outdoor** ، **Loose tube** نیز گفته می شود.

در این نوع کابل، هسته یا هسته های فیبر نوری در یک تیوپ پلاستیکی طوری قرار می‌گیرند که آزادانه امکان حرکت داشته باشند. این فضای خالی میان هسته ها و تیوپ، با یک نوع ژل به نام **Thixo tropic** پُر می‌شود، تا از نفوذ رطوبت جلوگیری شود.

به دلیل شناور بودن فیبرها درون تیوپ، این نوع کابل، در برابر نیروهای مکانیکی بیرونی، مقاوم است.

به همین دلیل معمولاً این کابل‌ها می‌توانند در مکانهای تحت فشار، به‌کار برده شوند.

دو نوع کابل **Loose Tube** وجود دارد:

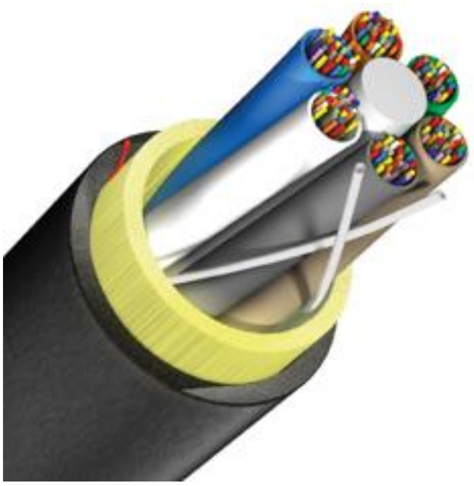
Central-Tube :

- این کابل ها، به منظور **Backbone** خارجی کاربرد دارند.
- نصب این نوع از کابل ها در داکت، تونل، تیوپ و شیارها آسان و سهل است.
- دارای یک لوله ی تو خالی است که فیبرهای نوری درون آن قرار دارند و اطراف آنها با ژل **Thixo tropic** پر شده است.
- بین لوله ی توخالیه حاوی فیبرهای شناور در ژل، و **Jacket** یک **Foil** آلومینیومی هم قرار دارد.

Stranded-Tube :

- این کابل ها نیز به منظور **Backbone** خارجی کاربرد دارند.
- نصب این کابل ها نیز در داکت، تونل، تیوپ و شیارها آسان و سهل است.
- دارای چندین لوله ی توخالی هستند که در هریک از آنها، چندین فیبر نوری قرار داشته و اطرافشان با ژل **Thixo tropic** پر شده است.
- بین خوشه ی تمام لوله های توخالی و **Jacket** ، یک **Foil** آلومینیومی هم قرار دارد.
- این کابل‌ها دارای عایقِ مقاومت مرکزی هستند که از پیچ خوردن یا خم شدنِ زیاد جلوگیری می کند.

Stranded Loose Tube



Central Loose Tube



❖ **Indoor & Outdoor** : برای هر دو محیط داخلی و خارجی کارآمد هستند، و ویژگی های مشترک با هر دو نوع کابل های داخلی و خارجی را دارند.

در جدول زیر بازه ی دمایی هر یک از انواع Jacket های کابل ارائه شده است:

Special High	Special Low	Normal High	Normal Low	Jacket
105˚C	-55˚C	80˚C	-20˚C	**PVC**
		80˚C	-60˚C	**PE**

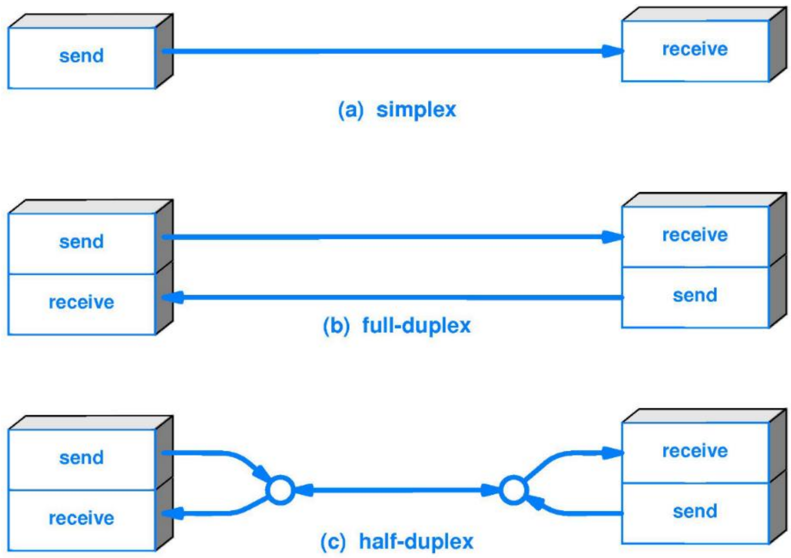
انواع فیبرنوری از لحاظ نوع انتقال اطلاعات:

- **Simplex** : فقط یک فیبر یا بستر انتقال دارد. یک سر آن فرستنده و سر دیگرش گیرنده است. و نکته ی مهم در مورد آن، این است که سر فرستنده و سر گیرنده، بطور ثابت تعریف شده اند و قابل جابجایی نیستند.

- **Full-Duplex** : شامل دو فیبر است که توسط یک لایه ی لاستیکی، به هم پیوسته می باشند. در هرسر این کابل، یک فرستنده داریم و یک گیرنده. به این مدل **bidirectional or BiDi transmission** نیز گفته می شود.

- **Half-Duplex** : کاملاً مشابه با کابل **Full-Duplex** است، اما انتقال داده ی طرفین نمی تواند همزمان انجام بگیرد. در هر زمان فقط یکی از طرفین می تواند دست به انتقال اطلاعات بزند. از یک کابل **FDX** می توان به عنوان **HDX** نیز استفاده کرد.

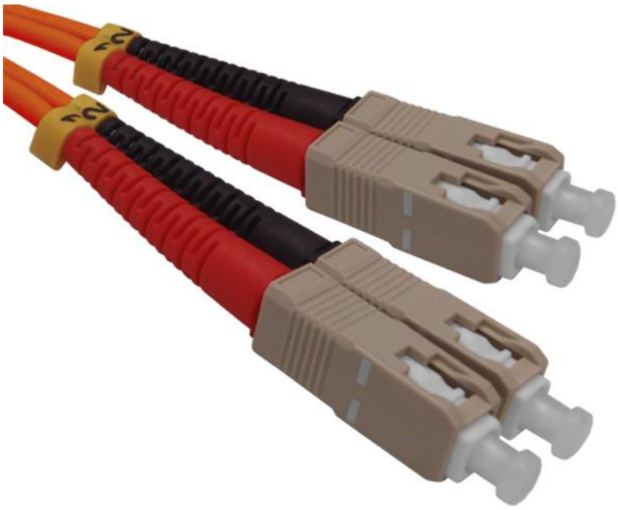
از هر دو نوع فیبرهای **Simplex** و **Half-Duplex** می توان هم در کابل های **Single Mode** و هم **Multimode** استفاده کرد، چون فقط با یک فیبر، قادر به عملیات انتقال هستند.



➢ Fiber Cable Terminals :

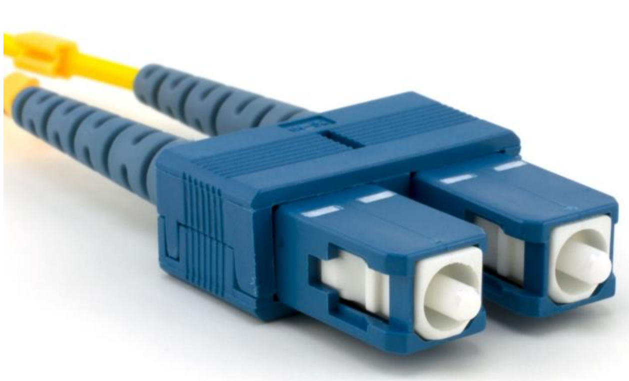
به ترمینال کابل نوری، **Coupler** یا **Adapter** گفته می شود، و یکی از انواع زیر می باشد:

- **LC Connector**



- **SC Connector**

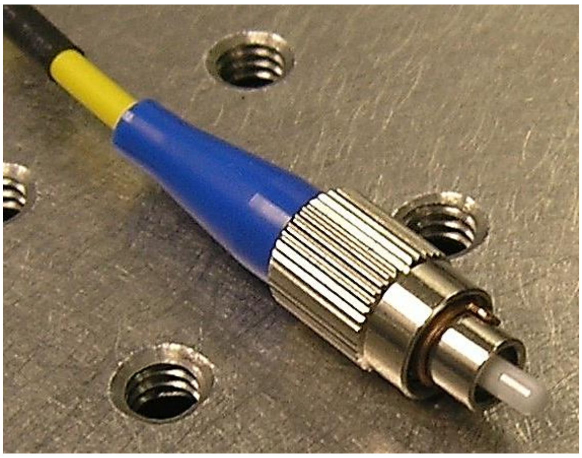




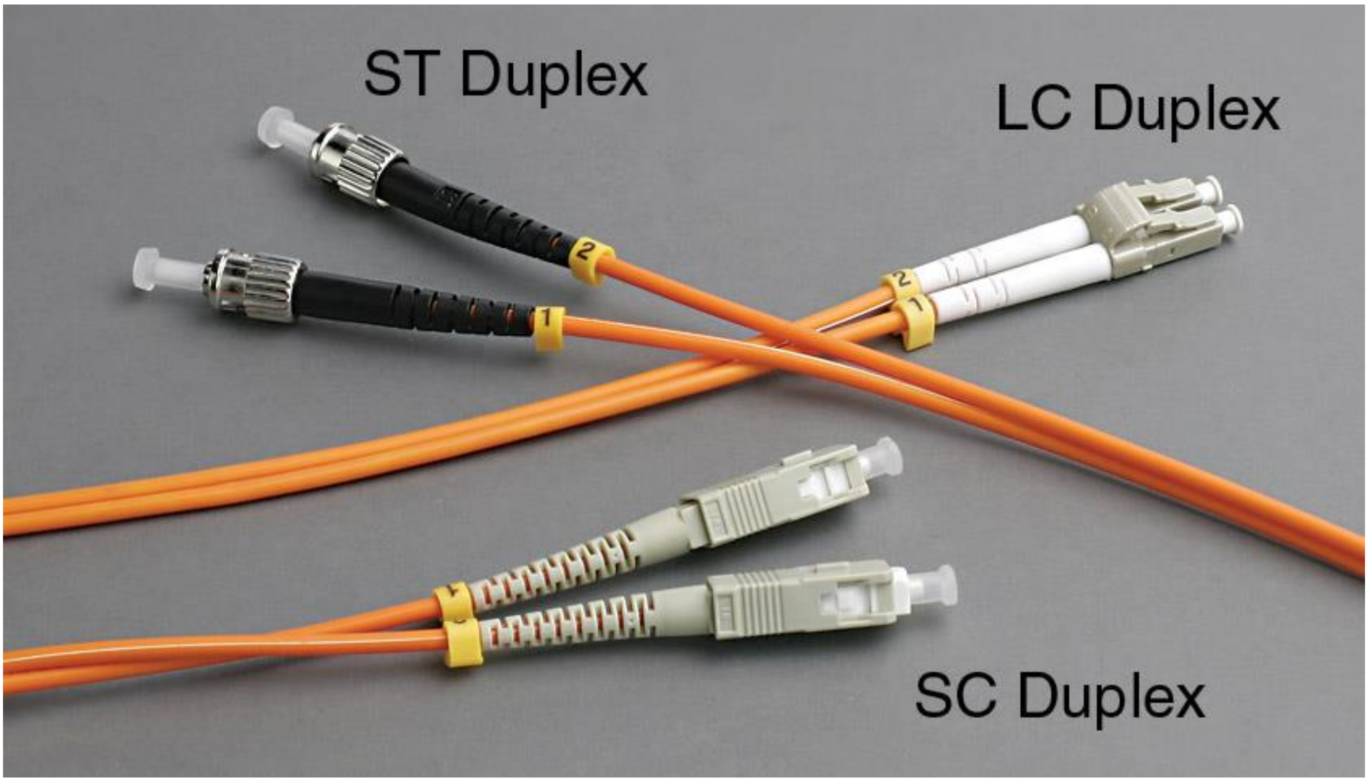
- **ST Connector**



- FC Connector







- Adapter ها شکل های متفاوتی دارند، اما عملکرد یکسانی دارند.
- Adapter های Single mode را می توان برای کابل های Multimode نیز استفاده کرد، اما برعکس، نمی شود.

➢ SFP and Gbic :

بطورمعمول، برای اتصال کابل هایی که نیاز به انتقال **data** با سرعت بالا دارند، مثل فیبرنوری، از یک **Connector** استفاده می شود به نام **Gbic** (Gigabit interface converter)، که دارای تکنولوژی ها و انواع مختلفی می باشد.

- بطورکلی، ماژول های **Gbic** قادر به پشتیبانی **network protocol** های زیر هستند:
  - ✓ Ethernet
  - ✓ Fast Ethernet
  - ✓ Gigabit Ethernet
  - ✓ Fibre Channel

- تکنولوژی های مورد استفاده در **Gbic** ها، **SFP** و **XFP** و **SFP+** هستند که تا سرعت های زیر قادر به ارسال و دریافت می باشند.
  (**S**mall **F**orm-Factor **P**luggable)

SFP : 4.25 Gb/sec
XFP : 10 Gb/sec
SFP + : 16 Gb/sec

- اما در گذشته که تکنولوژی های بالا وجود نداشت، از ماژول **Gbic** بطوراختصاصی برای اتصال کابل های فیبرنوری استفاده می شد، که دارای سرعت های 10 Mbps و 100 Mbps و 1 Gbps می بود.



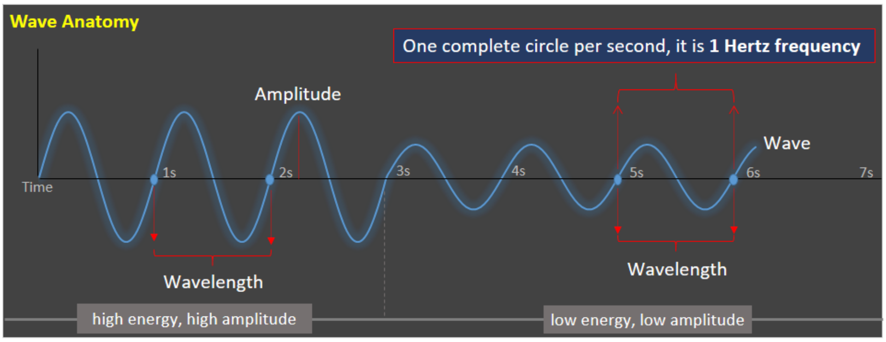
اما با ظهور تکنولوژی های بالا، اندازه ی **Gbic** کوچکتر و باریکتر شد و با افزودن این تکنولوژی ها، ماژول های **Gbic** امروزی ظاهر شدند که **mini-Gbic** نامیده می شوند؛ که به سادگی برای اتصال های **Switch** ها به یکدیگر و یا اتصال **Switch** ها به **Server** ها استفاده می شود، چه توسط کابل **TP** و چه توسط کابل **Fibre Channel**.

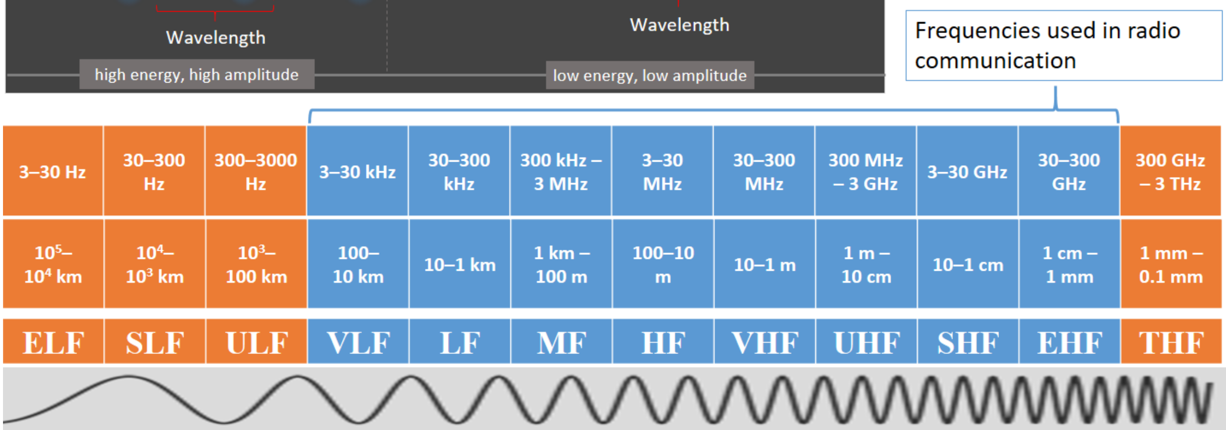
نکته: برای اتصال کابل های فیبر نوری که مجهز به یکی از Connector های Gbic هستند، نیازی به Patch panel نیست.

نکته: در صورت استفاده از هریک از ماژول های SFP در شبکه، جدا از اینکه کابل نوری باشد یا زوج سیم، قابلیت Hot-swappable دارند.

:Wireless Network

- می دانیم که در دنیا، نوعی از انرژی، به شکل امواج وجود دارد، که به آن، موج اکترومغناطیسی می گوییم.
- می دانیم که می توانیم امواج الکترومغناطیس را به کنترل و خدمت بگیریم.
- به دلیل شدت و ضعف در حالت های مختلفی که موج الکترومغناطیسی دارد، آن را در چندین بخش، دسته بندی می کنند.
- یکی از این بخش ها، **بخش امواج رادیویی** می باشد، در این دسته، موج الکترومغناطیسی، دو ویژگی دارد:
  - دیده نمی شود.
  - برای سلامتی انسان، خطرناک نیست.
- از امواج رادیویی به سادگی، جهت ارسال و دریافت «اطلاعات سیگنال شده»، استفاده می شود.
- ما می توانیم امواج رادیویی را توسط قطعه ای به نام آنتن، در جهات مختلف، در محیط منتشر کنیم و توسط یک آنتن دیگر، آنها را دریافت کنیم.
- امواج رادیویی در هوا با سرعتی حدود سرعت نور منتقل می شوند، پس سرعت انتقال زیادی را خواهیم داشت.
- بطورکلی، واحد اندازه گیری امواج الکترومغناطیسی، **Hertz** می باشد که به صورت **Hz** نشان داده می شود. (**measured in Hertz**)
  مقدار یک هرتز، برابر است با تعداد موج هایی که در یک ثانیه تولید می شوند، که این مقدار، با نام فرکانس شناسایی می شود.
- طیف یا گستردگی امواج رادیویی، از 3 Kilo Hertz تا 300 Giga Hertz می باشد.





مشخصات این باند های فرکانسی، که با حروف مخفف نشان داده شده اند، در جدول زیر، لیست شده اند:

فرکانس	طول موج	جزو دسته ی	مخفف نام دسته
3-30 Hz	10^5-10^4 km	Extremely low frequency	ELF
30-300 Hz	10^4-10^3 km	Super low frequency	SLF
300-3000 Hz	10^3-100 km	Ultra low frequency	ULF
3-30 kHz	100-10 km	Very low frequency	VLF
30-300 kHz	10-1 km	Low frequency	LF
300 kHz - 3 MHz	1 km - 100 m	Medium frequency	MF
3-30 MHz	100-10 m	High frequency	HF
30-300 MHz	10-1 m	Very high frequency	VHF
300 MHz - 3 GHz	1 m - 10 cm	Ultra high frequency	UHF
3-30 GHz	10-1 cm	Super high frequency	SHF
30-300 GHz	1 cm - 1 mm	Extremely high frequency	EHF
300 GHz - 3 THz	1 mm - 0.1 mm	Tremendously high frequency	THF

- از آنجایی که ارتباط توسط امواج رادیویی، بدون سیم، و به کمک امواج نامرئی انجام می شود، به این ارتباطات، **Wireless** گفته می شود.
- دستگاه‌های **wireless**، نیازی به پورت نداشته و تنها کافی ست مجهز به آنتن باشند.
- سازمانی که فرکانس های امواج **Wireless** را نظارت و بررسی می کند، **ITU** (International Telecommunication Union) می باشد.
- شرکت **IEEE** مسیول تنظیم و ثبت استانداردهای ارتباط **Wireless** می باشد.

- قابلیت استفاده از ارتباطات **Wireless** در سیستم های کامپیوتری، با نام **Wi-Fi** شناخته می شود که نام استانداردِ ثبت شده اش، **802.11** است.
- کلمه ی **WiFi**، مخفف نیست، و تنها یک نام استعاری است که در ابتدا به شکل **hi-fi** بوده است.
- دستگاه هایی که دارای امکانات و قابلیت های مطابق با استاندارد **IEEE802.11** هستند، نشان **Wi-Fi Certified** دریافت می کنند.
- **Access Point** یک دستگاه مرکزی است که در لایه ی دو (Data Link) کار می کند و کاری مشابه به **Switch** را انجام می دهد، با این تفاوت که **Access Point**، سیگنال های اتصال به شبکه ی کامپیوترها را در محیط منتشر می کند.
- امروزه تقریباً همه ی **Switch** ها و **Modem** ها و **Router** ها، بطور پیشفرض، تنظیمات سخت افزاری و نرم افزاری **Wireless** را نیز دارا هستند و قابلیت **WiFi** را ارائه می دهند.

✓ یکی از مهمترین مزیت های سیستم های رادیویی، کاهش حجم اتصال ها و سیم کشی ها می باشد.
✓ ارتباط به وسیله امواج رادیویی، بر پایه ی قوانین فیزیک است که باید آنها را در محاسبات و طراحی ها لحاظ کرد.
✓ می دانیم که اطراف ما امواج رادیویی بسیاری با فرکانس ها و طول موج های متفاوت وجود دارند.

در هر کشور باند های فرکانسی مختلف برای انجام امور خاصی در نظر گرفته می شوند. (frequency bands)
برخی از این باند های فرکانسی برای پخش های عمومی مثل تلویزیون و رادیو، و برخی دیگر برای ارتباط بین افراد و برخی برای ارتباط بین کشتی ها و هواپیما ها و برخی هم برای استفاده های دیگری اختصاص داده می شوند.
برای استفاده از باند های فرکانسی با کاربرد های خاص، نیاز به دریافت مجوزِ بهره برداری و استفاده از آنها از سوی نهاد های نظارتی می باشد.
مثلاً در ایران: سازمان تنظیم مقررات و ارتباطات رادیویی

در این میان، باند فرکانسی هم وجود دارد که برای استفاده های صنعتی، پزشکی و علمی از آن استفاده می شود و نیاز به دریافت مجوز ندارد.

- به این باند فرکانسی، **ISM Band** (پهنای باند صنعتی، علمی و پزشکی) گفته می شود. (Industrial, Scientific, Medical)
- موسسه ی **FCC** این محدوده ها را مشخص و استانداردسازی کرده و می کند.
- درحقیقت، ISM Band در محدوده ی **UHF** قرار داشته و از **سه محدوده** ی آن در **WiFi** (**902** MHz تا **5875** MHz) استفاده می شود.
- طبقه بندی باند فرکانسی **ISM** در ایران، به شکل زیر می باشد:

محدوده فرکانسی	فرکانس مرکزی
6765 - 6795 KHz	6780 KHz
433.05 – 434.79 MHz	433.92 MHz
61 - 61.5 GHz	61.25GHz
122 – 123 GHz	122.5 GHz
244 – 246 GHz	245 GHz
13553 – 13567 KHz	13560 KHz
26957 – 27283 KHz	27120 KHz
40.66 – 40.70 MHz	40.68 MHz
902 – 928 MHz	915 MHz
2400 – 2500 MHz	2450 MHz
5725 – 5875 MHz	5800 MHz
24 – 24.25 GHz	24.125 GHz

چون کمتر از ۱ گیگاهرتز هستند، به آنها ISM SubGHz نیز گفته می شود.

از پر مصرف ترین محدوده فرکانسی برای ارتباط بی سیم و انتقال داده می باشند. طوری که اکثر ماژول های بی سیم، تبادل داده و ارتباطات رادیویی موجود در بازار، این محدوده فرکانسی را پوشش می دهند.

سیستم WiFi درشبکه ها، از این دو محدوده استفاده می کند.
2.4GHz
5GHz

نکته: امروزه استفاده از محدوده ی 902 MHz تا 928 MHz در WiFi منسوخ شده است.

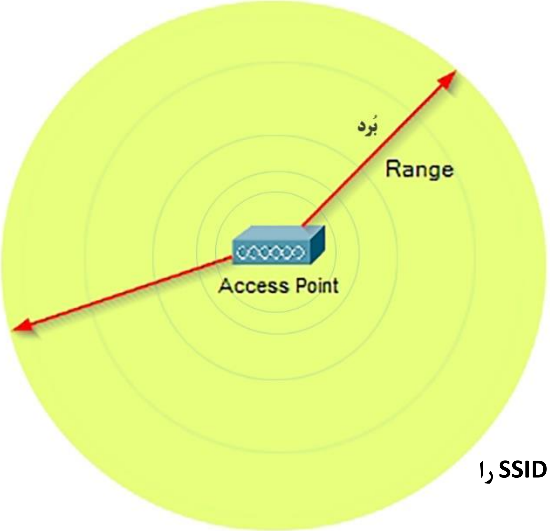
از طیف فرکانسی ISM SubGHz در کاربرد هایی که به بُرد بالا (High range) و پهنای باند کم (low bandwidth) نیاز باشد، استفاده می شود.
همچنین در کاربردهایی که نرخ تبادل اطلاعات در آن پایین می باشد، از این محدوده استفاده خواهد شد.

: WiFi Terms

- بُرد یا Range سیگنال، شعاعِ انتشار سیگنال‌های منتشر شده توسط Access Point است.

- بطور معمول، سیگنال های WiFi منتشر شده از Access Point تا فاصله ی 45 متری از آن، مؤثر و کاربردی هستند. که البته یک Access Point ایده آل و قدرتمند، قادر است تا فاصله ی 90 متری یا حتی بیشتر هم سیگنال ها را به خوبی ارسال کند.

- BSS: درحقیقت، وقتی تمام فضای اطراف یک AP را تا سقف میزان Range آن، به شکل فیزیکی متصور شویم، می بینیم که این فضای قابل پشتیبانی توسط امواج آن، به شکل یک کُره است. به این فضای کرویِ حول AP، گفته می شود: Basic Service Set .



- BSSID: درحقیقت، هر AP، توسط آدرس سخت افزاری خودش، شبکه اش را در محدوده ی BSS اش، تبلیغ می کند. پس به Mac address مربوط به یک AP، BSS ID گفته می شود.

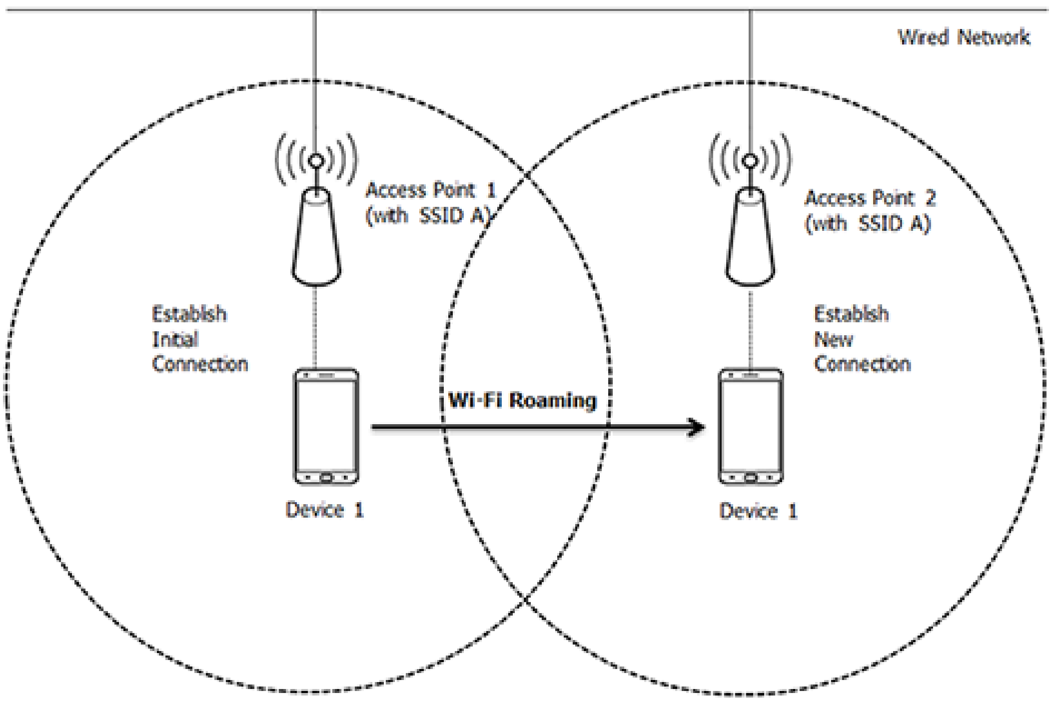
- SSID: درحقیقت، یک AP، دارای یک نام شناسایی هم هست، تا Client ها، به کمک این نام، آنها را شناسایی کنند، به این نام Service Set Identifier گفته می شود. یک AP می تواند بیش از یک SSID داشته باشد.

- DS: به شبکه ی wired ای که یک AP توسط uplink اش به آن متصل است، Distribution System گفته می شود.

- ESS: به مجموعه ای از AP ها که به یک DS متصل بوده و یک شبکه ی WiFi با یک SSID را تبلیغ می کنند، Extended Service Set گفته می شود.

- Roaming:

وقتی در یک شبکه، یک WiFi Client، از محدوده ی Range یک Access Point خارج شده و به Range یک AP دیگر وارد می شود، لازم است که ارتباط Client با شبکه، همچنان پابرجا و بدون کوچکترین قطعی ادامه داشته باشد.
به فرآیند منتقل کردن «اتصال–Client –به–شبکه» از AP اول به AP دوم، Roaming گفته می شود.



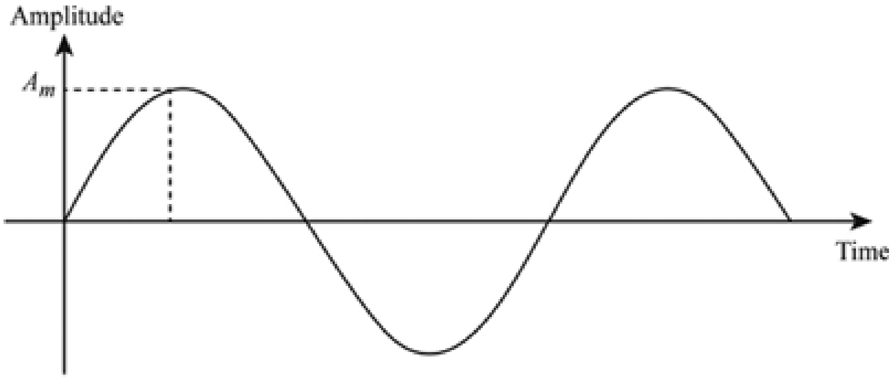
:Modulation

به فرآیندی که بتوان، اطلاعات را در بستر امواج رادیویی ارسال و دریافت کرد، یا به عبارتی اطلاعات را روی امواج سوار کرد، **تلفیق در امواج** یا **Modulation** گفته می شود.

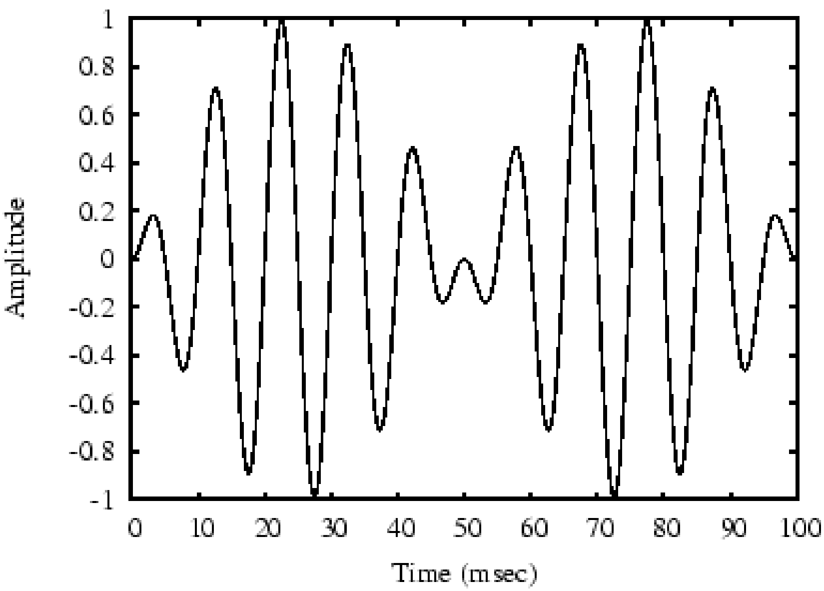
امواج الکترومغناطیسی، چهار مشخصه دارند، که برای فهماندن اطلاعاتی که داریم به این امواج (**Modulation**)، از آن چهار ویژگی استفاده می کنیم.

- ✓ پس سوار کردن اطلاعات، به شکل سیگنال های امواج الکترومغناطیسی، به کمک چهار مشخصه ی امواج انجام می شود.
- ✓ ما می توانیم این تلفیق داده در موج را، با تغییر یکی یا تعدادی و یا همه ی چهار ویژگی موج، انجام دهیم.
- ✓ درحقیقت، وقتی داده ای را روی یک موج الکترومغناطیسی تلفیق می کنیم، به آن موج، **Signal** گفته می شود.

در شکل زیر، یک موج الکترومغناطیسی ساده را مشاهده می کنیم:

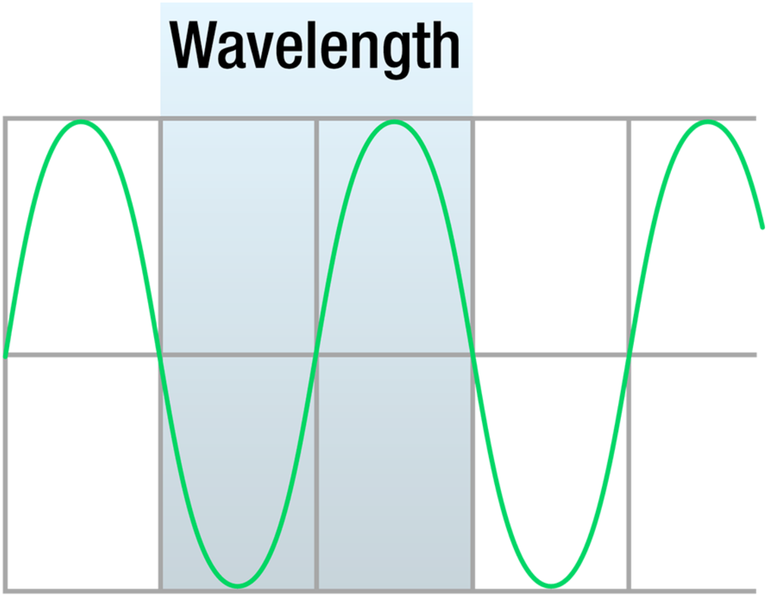


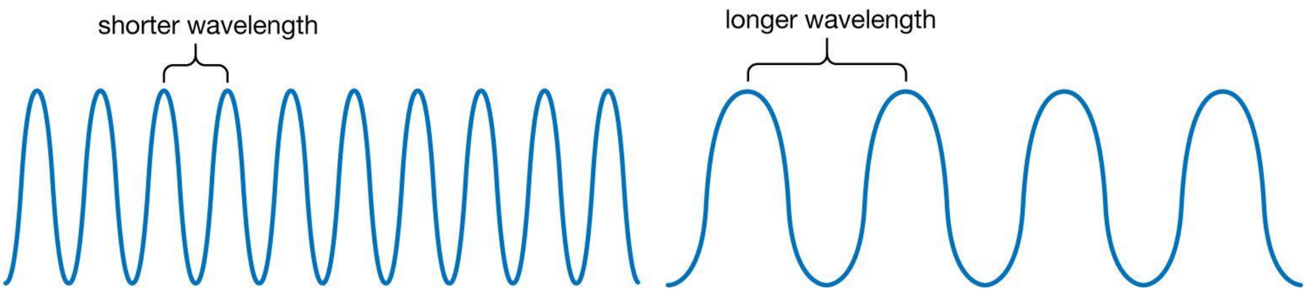
در شکل زیر، یک موج الکترومغناطیسی دستکاری شده را مشاهده می کنیم، که عملن به این موج، **Signal** گفته می شود:



➢ Wavelength:

واحد اندازه گیری طول هریک موج الکترومغناطیسی، متر است. (measured in Meter)





➢ Frequency:

درحقیقت، فرکانس سیگنال‌های مورد استفاده در شبکه های WiFi ، عبارتند از :

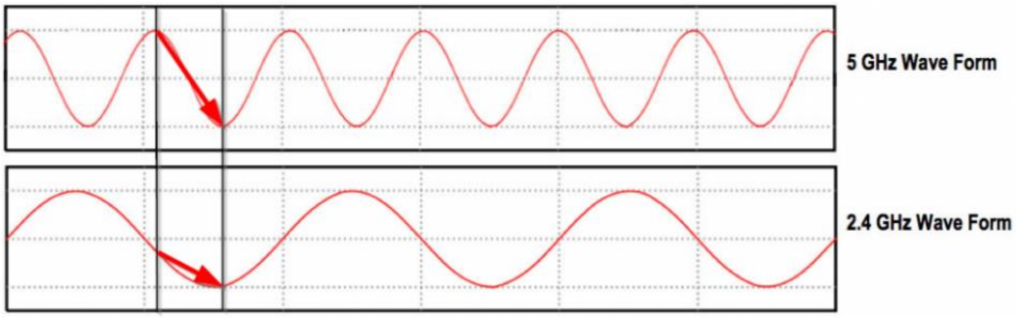
- **2.4 گیگاهرتز،**
- **5 گیگاهرتز،**

در حال حاضر 2.4 GHz با اینکه سرعت پایین تری دارد، محبوب ترین فرکانس مورد استفاده در دستگاه ها و لوازم بی سیم است.
از طرف دیگر، فرکانس 5 GHz سرعت بیشتری دارد، (higher speed) اما بُرد کمتری نسبت به 2.4 دارد. (shorter range)

مقدار طول موج، رابطه ی کاملاً برعکسی با مقدار فرکانس دارد.

- هرقدر فرکانس کمتری داشته باشیم، طول موج بلندتر خواهد بود،
- هرقدر طول موج بلندتر باشد، ساده تر قادر به نفوذ به و عبور از اشیا، و در نتیجه طی کردن مسافت بیشتر، خواهد بود.
- هرقدر مقدار فرکانس بیشتر باشد، حجم داده های بیشتری را می توان در زمان کوتاه تری انتقال داد، به عبارتی سرعت ارتباط بیشتر می شود.

✓ به Router هایی که تنها، یکی از باندهای 2.4GHz یا 5GHz را پشتیبانی می کنند، **Single band router** گفته می شود.
✓ به Router هایی که هر دو باند 2.4GHz و 5GHz را پشتیبانی می کنند، **Dual band router** گفته می شود.



اگر در یک محیط بزرگ زندگی می‌کنید و خانه‌ای دارید که متراژ بالایی دارد و دیوارهای زیادی نیز بین شما و مودم قرار گرفته‌اند، در این صورت، استفاده از فرکانس 2.4 گیگا هرتزی بهتر خواهد بود.

نکات:

✓ درحقیقت، نه فقط دستگاه های شبکه مثل Access Point و Router، بلکه دستگاه های دیگری مثل ماکروویو و تلفن های خانگی، از فرکانس 2.4GHz استفاده می کنند، که این می تواند شبکه را دچار اختلال کند، چراکه این محدوده ی فرکانسی در محیط موردنظر، شلوغ خواهد شد، که منجر به تداخل سیگنال های متفاوت با یکدیگر می شود، به همین جهت بود که استفاده از محدوده ی 5GHz نیز پدید آمد.
✓ فرض کنید بیش از یک AP در یک محیط داشته باشیم، یکی از بهترین راهکارها جهت کاهش Noise، تنظیم آنها در Channel های متفاوت است.
✓ بر روی بیشتر Router ها، گزینه ی Channel، بر روی حالت خودکار تنظیم می باشد.
✓ می دانیم که بعضی کانال ها، سریع‌تر هستند، ولی این به این معنا نیست که حتما بهترین انتخاب هستند.
✓ اگر در یک محیط خیلی متراکم و شلوغ، بیش از سه AP داشته باشیم، استفاده از فرکانس 5GHz منطقی تر خواهد بود.

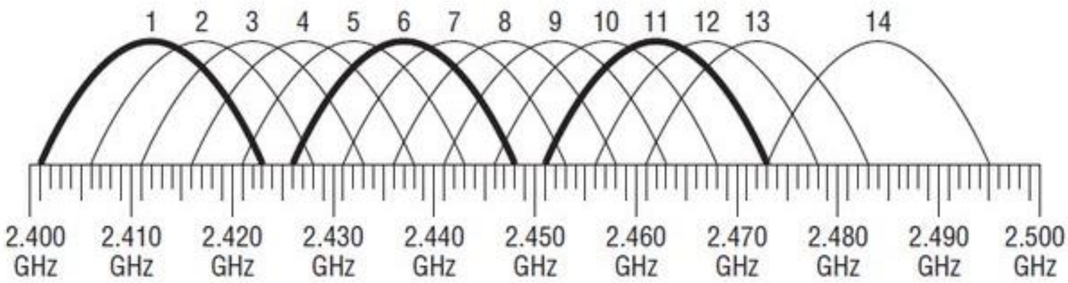
فرکانس 2.4GHz :

- طول موج این محدوده ی فرکانسی، 4.92 اینچ می باشد.
- وقتی می گوییم، فرکانس برابر با **2.4** گیگاهرتز است، یعنی در یک ثانیه، **2.4 میلیارد** موج، تولید و ارسال می شود.
- پس با ضرب این تعداد موج در طول موجی که گفته شد، مشخص است که مثل نور، در یک ثانیه **300** هزار کیلومتر را طی می کند.

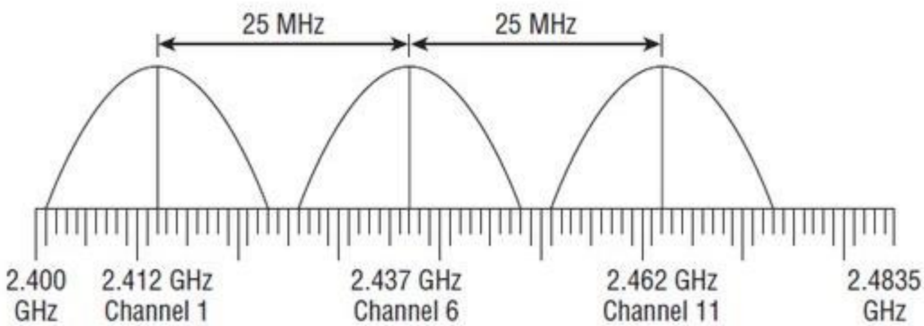
اما درحقیقت، فرکانس 2.4 GHz به شکل کاملاً دقیق استفاده نمی شود، بلکه این، یک محدوده یا باند است، از 2.40 GHz تا 2.50 GHz

این محدوده را به محدوده هایی کوچکتر تقسیم می کنیم، که به هریک از آنها، کانال فرکانسی (Frequency channel) **گفته می شود.**

- فرکانس میانی هر کانال را، به عنوان، فرکانس پایه ی آن، یا F_0 در نظر می گیریم.
- پس باند فرکانسی **2.4GHz** دارای **14** کانال خواهد بود، که فاصله ی میان F_0 دو کانال مجاور، فقط 5 MHz خواهد بود!



- جهت جلوگیری از بروز اختلال (Overlapping) میان کانالهایی که استفاده می کنیم، باید فاصله ی میان F_0 آنها، **حداقل** 20 MHz باشد، که درنتیجه بهترین کانال ها جهت استفاده، یک و شش و یازده خواهند بود. (**3** non-overlapping channels)
- همانطور که در شکل زیر می بینیم، خواه ناخواه، فاصله ی میان هردو کانال مجاور از این سه کانال، برابر با **25 MHz** خواهد بود.



- پس همانطور که می بینیم، هر کانال فرکانسی در محدوده ی خودش، **22** فرکانس را پشتیبانی می کند.
- یعنی فضای قابل پشتیبانی برای هر کانال در استاندارد **2.4GHz**، یک محدوده ی حداکثر **22** مگاهرتزی خواهد بود.

ISM 2.4 – 2.5 GHz [2400 MHz – 2500 MHz]					
Channel	F_0 (GHz)	**Frequency range** (MHz)	Use in **most of the world**	Use in **North America**	Use in **Japan**
1	**2.412**	2401–2423	Yes	Yes	Yes
2	**2.417**	2406–2428	Yes	Yes	Yes
3	**2.422**	2411–2433	Yes	Yes	Yes
4	**2.427**	2416–2438	Yes	Yes	Yes
5	**2.432**	2421–2443	Yes	Yes	Yes
6	**2.437**	2426–2448	Yes	Yes	Yes
7	**2.442**	2431–2453	Yes	Yes	Yes
8	**2.447**	2436–2458	Yes	Yes	Yes
9	**2.452**	2441–2463	Yes	Yes	Yes
10	**2.457**	2446–2468	Yes	Yes	Yes
11	**2.462**	2451–2473	Yes	Yes	Yes
12	**2.467**	2456–2478	in low-power mode Yes	in low-power mode Yes	Yes
13	**2.472**	2461–2483	in low-power mode Yes	in low-power mode Yes	Yes
14	**2.484**	2473–2495	No	No	Yes

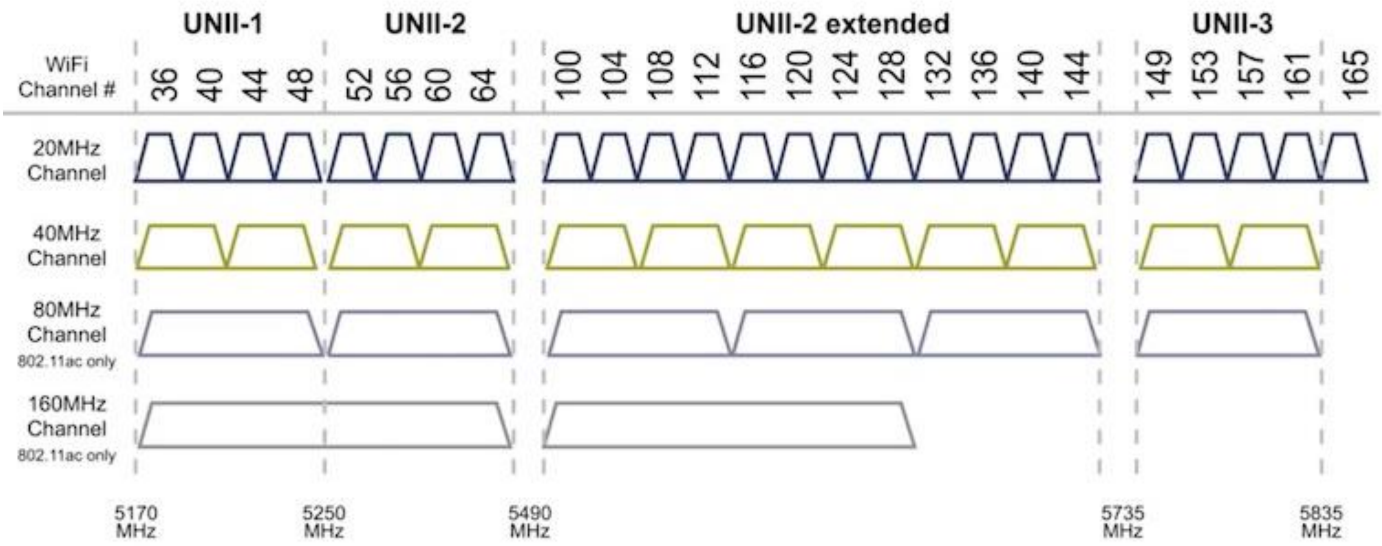
فرکانس 5GHz :

طول موج در این محدوده ی فرکانسی، 2.03 اینچ می باشد.

این باند فرکانسی:

- طیف وسیع تری دارد.
- نیاز به **Power** بیشتری جهت ارسال سیگنال دارد.
- تعداد کانال های آن، در کشورهای مختلف، متفاوت خواهد بود. مثلاً در **USA**، تعداد کانالهای قابل استفاده در این فرکانس، **25** کانال خواهد بود. (**25** non-overlapping channels)
- فاصله ی هرکانال، با کانال مجاورش طوری تعریف شده است، که هیچ همپوشانی رخ نخواهد داد.
- بطورکلی، کانال ها در این باند فرکانسی، در چهار دسته (تحت نام **U**nlicensed **N**ational **I**nformation **I**nfrastructure)، تفکیک می شوند:
  - U-NII 1
  - U-NII 2A
  - U-NII 2C Extended
  - U-NII 3

- پهنای باند هر کانال و درنتیجه تعداد کانال ها در هر دسته، می تواند بسته به نوع استاندارد **WiFi** مورد استفاده، متفاوت باشد:



نکات:

- می بینیم که در این فرکانس، شماره ی کانال ها از 36 شروع شده و چهار واحد-چهار واحد افزایش می یابد.
- درحقیقت فضای قابل پشتیبانی برای هر کانالِ فرکانسیِ 2.4GHz، برابر با 22 MHz خواهد بود؛ در حالی که این فضای قابل پشتیبانی تحت فرکانس 5GHz ، حداقل 20 MHz است، که تا امروز، می توان آن را تا 160 MHz نیز افزایش داد.

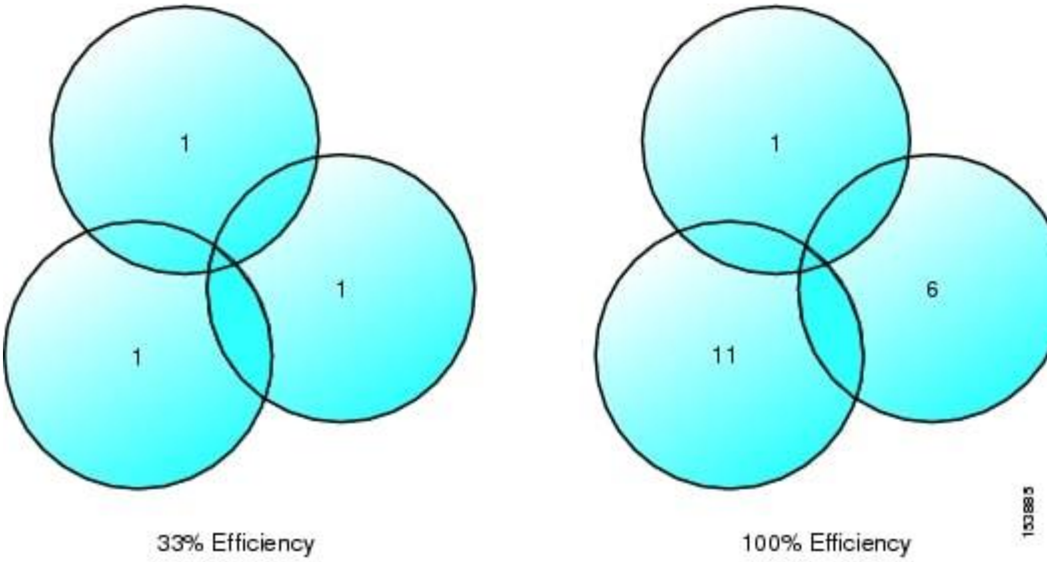
- **کانال های مربوط به U-NII 2 و UNII 2 Extended، رزرو شده اند که آنها را با DFS** (Dynamic Frequency Selection) **نشان می دهند.**
- **کانال های DFS، برای استفاده ی موارد ضروری مثل ارتباطات بی سیم آمبولانس، پلیس و ... رزرو شده اند، یعنی می توان به عنوان یک Client شخصی، به آنها وصل شد، اما اگر موردی پیش بیاید که پلیس یا آمبولانس نیاز به اتصال داشته باشد، پس در اولویت تر بوده و client بطورخودکار، ارتباطش را از دست خواهد داد.**
- **بهترین کانال های قابل اطمینان جهت استفاده در شبکه ی سازمان، U-NII-1 و U-NII-3 می باشند.**

Channel Number	Frequency (MHz)	Europe (ETSI)	North America (FCC)	Japan
36	5180	Indoors	✓	✓
40	5200	Indoors	✓	✓
44	5220	Indoors	✓	✓
48	5240	Indoors	✓	✓
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✓	No Access
153	5765	SRD	✓	No Access
157	5785	SRD	✓	No Access
161	5805	SRD	✓	No Access
165	5825	SRD	✓	No Access

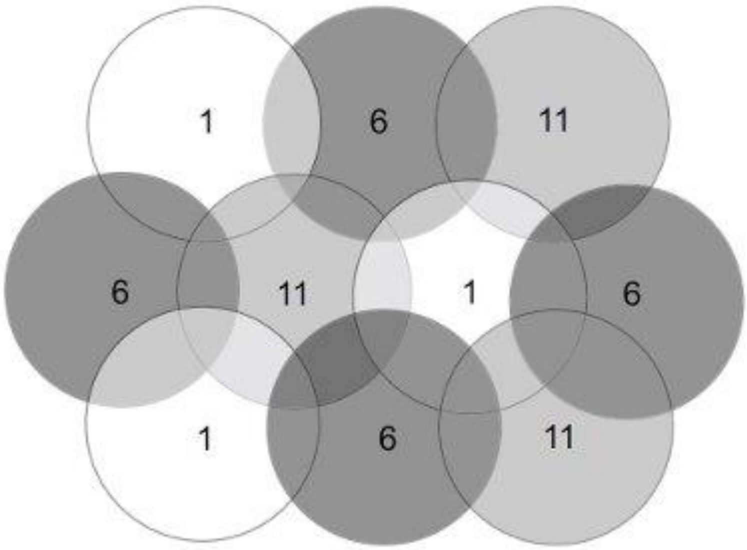
:Channel design

فرض کنید، در یک محوطه، نیاز به نصب و راه اندازی چند AP، برای انتشار و تبلیغ شبکه داشته باشیم.
پس لازم است که طراحی و فواصل میان آنها را به درستی انتخاب کرده و انجام دهیم.

نکته: درحقیقت باید توجه کنیم که اگر همه ی AP ها در یک Channel باشند نیز، شبکه همچنان کار می کند، اما در برخی نقاط، با بازدهی خیلی کمتر.



پس Access Point ها را به شکل زیر، در کانال های متفاوت از کانال AP های مجاور، تنظیم می کنیم:



اگر بین دو AP، یک دیوار آجری موجود باشد، پس هر دو می‌توانند بدون هیچ تداخلی از یک کانال یکسان استفاده کنند؛
ولی اگر دیوار نازک باشد یا پنجره‌های زیادی داشته باشد، لازم است که از کانال‌های مختلف استفاده کنیم.

در حقیقت در تمام شرایط، کانال بندی ها را طوری انتخاب می کنیم، که هیچ دو AP مجاوری، در یک کانال یکسان فعال نباشند، اما گاهی جهت جلوگیری از بروز Dead Zone، باید فاصله ها و تنظیمات AP ها را طوری انجام دهیم که دچار همپوشانی (overlapping) شوند، تا کاربر در تمام محیط موردنظر، دچار قطعی یا کاهش کیفیت ارتباط نشود.

فرض کنید، در بخشی از شبکه مان، یک AP نصب کرده ایم که در نزدیکی آن، احتمال وجود یک AP از شبکه ی ساختمان همسایه وجود داشته باشد. اینکه کانال AP مجاور که مربوط به شبکه ی همسایه است، در چه کانالی است، و آیا واقعن AP ای وجود دارد یا خیر، را می توان توسط نرم افزارهایی که به رایگان در اینترنت می توان دریافت کرده و نصب کرد، بررسی و پیگیری کرد.

به سادگی می توان نرم افزارها یا Application هایی را با عنوان WiFi Scanner **یا** WiFi Analyser **و یا** WiFi Explorer **برای انواع سیستم عامل ها** (mac، Windows، Android و ...) **دریافت کرد.**

مثل نرم افزارهای:

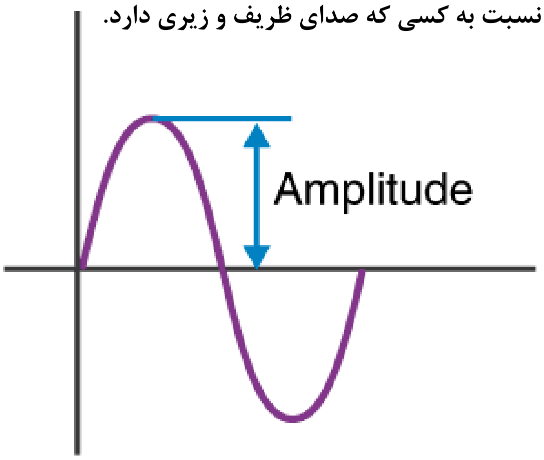
- **Homedale** و **WifiInfoView** که رایگان هستند،
- **Fing** که نرم افزار کارآمدی است، اما نسخه ی رایگان آن، محدودیت هایی دارد،
- **Acrylic WiFi Analyzer** که کاملاً حرفه ای و قدرتمند است، اما نسخه ی رایگان آن، محدودیت هایی دارد.

اینگونه نرم افزارها، به کمک کارت شبکه ی Wireless روی دستگاه شما، تمامی سیگنال های WiFi موجود در محیط پیرامون را بررسی و با مشخصات، لیست می کنند.
و به سادگی می بینیم که آیا AP ای در نزدیکی وجود دارد که روی Channel موردنظر کار کند یا خیر.
بطورمثال، اگر که سطح سیگنال یک AP دیگر که با سیگنال شبکه ی ما تداخل دارد، پایین باشد، می توان از آن چشمپوشی کرد.

اما نرم افزارهایی هم وجود دارند که به کمک آنها می توان، شبکه ی Wireless را به شکل تصویری و به کمک نمودارها و نقشه های گرافیکی، طراحی کرد. این نوع نرم افزارها را می توان با عنوان Wifi Network Heatmaps **جستجو کرد.**

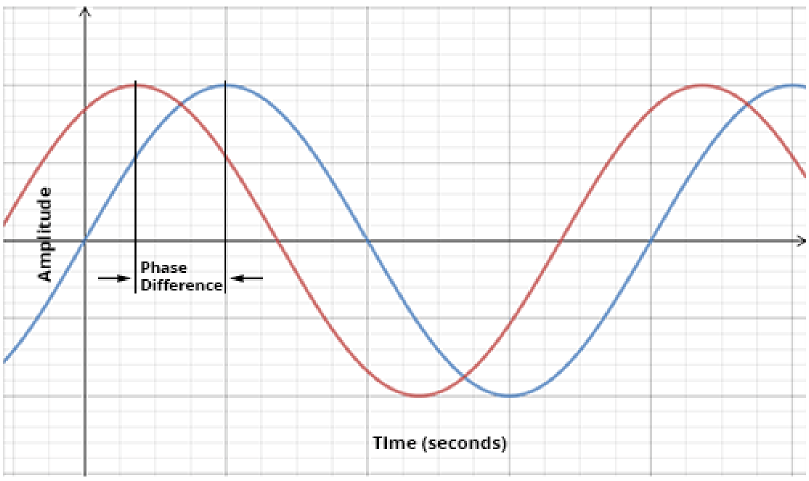
➢ :Amplitude

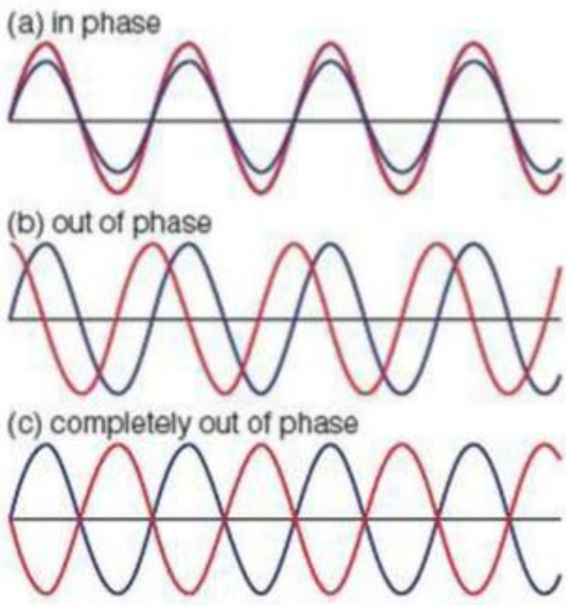
دامنه ی موج، مقدار ارتفاع آن موج، یا حداکثر فاصله ای ست که ذره ی موج، با خط محور مبدا، طی می کند.
بطورمثال،
موج صدای شخصی که فریاد می زند یا جیغ می کشد، دارای دامنه ی بلندتری ست از کسی که آرام حرف می زند.
موج صدای شخصی که با صدای زمخت و بم صحبت می کند، دارای فرکانس کمتری ست، نسبت به کسی که صدای ظریف و زیری دارد.



➢ :Phase

درحقیقت اینکه یک موج را، با دامنه ی صفر ارسال کنیم، و یا اینکه با یک دامنه ی غیر از صفر ارسال کنیم،
نتیجه ی متفاوتی را در مقصد خواهیم داشت.





: WiFi Architectures

بطورکلی، یک شبکه ی Wireless، می تواند شامل اعضای زیر باشد:

- ✓ Wireless Client
- ✓ Access Point
- ✓ Wireless Lan Controller

چهار نکته که باید قبل از راه اندازی شبکه ی Wireless آنها مشخص کنیم:

- ➢ **AP ها را باید به شکل مستقیم و یکی یکی پیکربندی کنیم، و یا به کمک یک دستگاه مرکزی** (WLC)
- ➢ **جهت اتصال به محیط پیکربندی AP ها، از محیط CLI استفاده می کنیم و یا از GUI.** (برخی AP ها تنها یکی و یا هردو را پشتیبانی می کنند.)
- ➢ **از کدام دستگاه یا تکنولوژی، جهت احراز هویت Client هایی که درخواست اتصال به AP ها را می دهند، استفاده کنیم.**
- ➢ **نحوه ی اتصال AP ها به سیستم distribution** (شبکه ی کابلی)

بطورکلی، معماری های شبکه های Wireless ، از لحاظ مدیریت و ارتباط AP ها با یکدیگر، در یکی از دسته های زیر قرار دارند:

- **Distributed**: دستگاه های Wireless، بر طبق یک ساختار، به یکدیگر متصل خواهند بود.
- **Centralized**: دستگاه های Wireless، به یک دستگاه کنترل کننده ی مرکزی، متصل هستند، و توسط آن با یکدیگر در ارتباط هستند.

  این دستگاه مرکزی، تعداد محدودی ارتباط با Client و تعداد محدودی ارتباط با AP ها را پشتیبانی می کند.

معماری های قابل راه اندازی در شبکه های بی سیم:

SOHO (Small Office/Home Office):

- **بطورمعمول، تنها یک SSID وجود دارد.**
- **تنها یک Router با قابلیت wireless و یا فقط یک اتصال بی سیم به یک AP وجود دارد، که Wlan را ارایه می کند.**

Autonomous:

- **در این مدل، هریک از AP ها، به تنهایی و مستقیم، پیکربندی می شود.**
- **در این مدل، باید به تنظیمات SSID ها دقت کنیم، که معمولن در سازمان ها، حداقل نیاز به دو SSID خواهد بود.**
  - وقتی بیش از یک SSID داشته باشیم، هریک از آنها را به یکی از VLAN ها اختصاص می دهیم،
  - بر روی هر AP، همه ی VLAN ها، تحت یک Wireless Channel کار خواهند کرد؛ پس گاهی میان Client ها، افت سیگنال رخ می دهد.
  - جهت اتصال به تنظیمات خود AP ها، نیاز به یک VLAN دیگر می باشد، که IP خود AP جزء این VLAN خواهد بود. (Management Vlan)
- **نکاتی که باید بر روی AP تنظیم کنیم:**
  - RF Channel (5GHz / 2.4 GHz)
  - Transmit power
  - Client Authentication Method
  - How to setup QoS
  - How to bridging into the wired distribution system
  - Create SSIDs and VLANs
- **این معماری، برای استفاده در شبکه های کوچک، کاربرد دارد. شبکه های تحت این معماری، به سادگی قابل گسترش (scalable) نیستند.**

مشکل این روش:

- **درصورت بیشتر بودن تعداد SSID ها، تعداد VLAN ها نیز بیشتر خواهد شد، و باید بر روی همه ی AP ها، به شکل دستی، همه ی SSID ها و سپس VLAN ها و سپس اتصال آنها را راه اندازی کنیم.**
- **نظارت و مقابله با نفوذهای خارجی، بسیار مشکل و در صورت بیشتر شدن AP ها، غیرممکن خواهد شد.**

Enterprise Design:

- **این معماری، برای شبکه های بزرگتر کاربرد دارد، و به سادگی scalable می باشد.**
- **جهت انجام پیکربندی موردنظر و ارسال update های سیستم عامل یا Firmware به AP ها، از WLC استفاده می شود.**
- **همه ی AP ها، بطورمداوم وضعیت خودشان و وضعیت Client های شان را به WLC گزارش می دهند.**
- **WLC یک محیط مدیریتی مرکزی برای AP ها می باشد.**
- **از آنجایی که در این مدل، نیازی به ارتباط مستقیم و پیکربندی دستی بر روی AP ها نیست، به AP های این مدل، Lightweight (LAP) گفته می شود.**

نکته: هنگام تهیه ی AP ها، باید به این نکته دقت داشت که قابلیت Lightweight را پشتیبانی کنند؛ چون هر AP ای این قابلیت را پشتیبانی نمی کند.

- **در این روش، WLC را در خود مکانی که شبکه را راه اندازی کرده ایم، راه اندازی می کنیم.** (On-Site deployment)
- **از مزایای استفاده از WLC:**
  - شناسایی AP هایی که BSS آنها با یکدیگر overlapping دارند، و تصحیح و تنظیم خودکار آن کانال ها.
  - شناسایی AP هایی که از کار افتاده اند و یا به هردلیلی از دسترس خارج شده اند،
  - نظارت و مدیریت ترافیک Client ها

Cloud-based:

- **کاملاً مشابه با حالت قبل است، با این تفاوت که در این روش، WLC را در یک محیط ابری، راه اندازی می کنیم.**
- **Cloud می تواند private و یا public باشد.**
- **در شبکه های CISCO، این بستر ابری، یک Public Cloud می باشد که توسط شرکت Meraki فراهم می شود.**
- **بطورکلی، این معماری CISCO، توسط Meraki Cloud پشتیبانی می شود.** (Cisco Meraki)
- **وقتی دستگاه ها به شبکه متصل می شوند، بطورخودکار تنظیم و پیکربندی و ثبت در Meraki Cloud و قابل استفاده خواهند شد.**

نکته: هنگام تهیه ی AP ها، باید به این نکته دقت داشت که قابلیت Lightweight را پشتیبانی کنند؛ چون هر AP ای این قابلیت را پشتیبانی نمی کند.

Split-MAC:

منظور از MAC همان Media Access Control در لایه دو مدل TCP/IP می باشد.

- **در این حالت، بخشی از وظایف به عهده ی خود AP و بخش دیگر، به عهده ی WLC خواهند بود.**

نکته: هنگام تهیه ی AP ها، باید به این نکته دقت داشت که قابلیت Lightweight را پشتیبانی کنند؛ چون هر AP ای این قابلیت را پشتیبانی نمی کند.

- **خود AP ها، وظایف لایه یکی و لایه دویی که نیاز به اعمال به موقع دارند را** (Real time funtions) **عهده دار می شوند. مثل:**
  - Frames Receive and Transmit : **مدیریت ارسال و دریافت Frame ها توسط سیگنال های Wireless**
  - MAC Management : **زمانبندی های موردنیاز جهت تخصیص یا سلب Channel**
  - Encryption : **رمزنگاری بسته های ارسالی و رمزگشایی بسته های دریافتی**
- **از وظایف WLC:**
  - Config type : Channel Selection | Transmit power | SSID | و ...
  - Roaming management : مدیریت جابجایی میان Channel ها و یا میان AP ها
  - Client Authentication
  - Security Policy Management
  - QoS Management
- **WLC می تواند، سخت یا نرم افزاری، تحت Cloud و یا locally باشد.**

Converged Wireless network:

جهت معرفی این مدل معماری شبکه های بی سیم، لازم است که ابتدا با پروتکل CAPWAP آشنا شویم:

➢ Access Point:

- دستگاهی که امواج wifi را در شبکه منتشر می کند، Access Point است که Client ها را به شبکه ی LAN وصل می کند.
- wifi یک فناوری لایه دویی می باشد جهت ایجاد پلی میان Client ها و LAN.
- AP ها، هیچ عملیات Routing ای انجام نمی دهند.
- در شبکه های کوچک، هر AP را بطورمستقل، مدیریت و مانیتور می کنیم.
- اما در شبکه های بزرگ، که بیش از ده ها AP وجود خواهند داشت، جهت جلوگیری از صرف وقت و هزینه ی زیاد، جهت اعمال هرگونه تغییر کوچک و بزرگ بر روی همه ی AP ها بطورهمزمان، از **Wireless LAN Controller** (WLC) استفاده می کنیم.
- **WLAN Controller** یک سیستم مدیریت مرکزی برای AP های موجود در شبکه می باشد که توسط آن می توان تغییرات، عیب یابی و نظارت کردن ها را به سادگی اعمال کرد.

نکته: درحقیقت یک AP:

- از سمت خارجی، ارتباطات را تحت پروتکل 802.11 مدیریت می کند،
- از سمت داخلی، ارتباطات را تحت پروتکل 802.3 مدیریت می کند.

از لحاظ فیزیکی، دو نوع AP وجود دارد:

- **Indoor AP:** که خود شامل چند نوع می باشد:
  - دیواری (In-wall AP)
  - سقفی (Ceiling AP)
  - رومیزی (Desktop AP)
- **Outdoor AP:**

از لحاظ کنترلپذیری و مدیریت، دو نوع AP وجود دارد:

- **Individually managed** (Autonomous یا خودمختار و یا Stand alone) :
  - درحقیقت کافی ست این نوع AP را فقط به Network وصل و روشن کنیم، سپس با انجام تنظیمات موردنیاز روی آن، Client ها می توانند به آن وصل شوند.
  - مناسب محیط های کوچک است.
- **Centrally managed** (Lightweight) :
  - در شبکه های بزرگ، که به ده ها یا صدها AP نیاز است، منطقی نخواهد بود که تنظیمات موردنیاز روی همه ی آنها را به شکل جدا جدا انجام دهیم، پس توسط دستگاه WLC، همه AP ها را به مدیریت در خواهیم آورد، که به این AP ها، Lightweight گفته می شود.
  - درحقیقت Lightweight ها هیچگونه قدرت مدیریتی نخواهند داشت؛ و همه ی تصمیم ها و مدیریت ها را WLC انجام و از طریق این AP ها، در شبکه اعمال خواهد کرد.

پیکربندی Access Point ها:

بسته به نوع و مدل یک AP، آن را به یکی از اشکال زیر می توان تنظیم کرد:

- ✓ از طریق GUI
- ✓ از طریق CLI
- ✓ از هر دو طریق بالا

جهت انجام اولین اتصال به یک AP و پیکربندیِ آن، یک کامپیوتر را توسط کابل Console به Console Port آن متصل می کنیم.

در زیر، تصویر یک Access Point شرکت Aruba را می بینیم که در بالا > درگاه Console آن که یک mini USB است، قرار دارد.



طبق شکل:

- **درگاه E1، جهت اتصال آن به شبکه ی کابلی استفاده می شود.**
- **درگاهی که با ولتاژ 12V مشخص شده است، جهت اتصال آداپتور برق آن است.**
- **اگر قرار است AP را به یک Interface روی Switch یا Router که قابلیت PoE را پشتیبانی می کند، متصل کنیم، پس نیازی به دو درگاه دیگر (12V و E1) نخواهد بود، و تنها کافی ست AP را توسط درگاه E0 به آن Interface متصل کنیم.**

نکته:

- **معمولن ارتباط میان AP با SW، بر روی حالت Trunk قرارخواهد داشت؛ که درنتیجه، uplink مربوط به SW نیز، Trunk خواهد بود.**
- **ارتباط میان AP با SW، توسط یک و یا حداکثر دو کابل خواهد بود.**

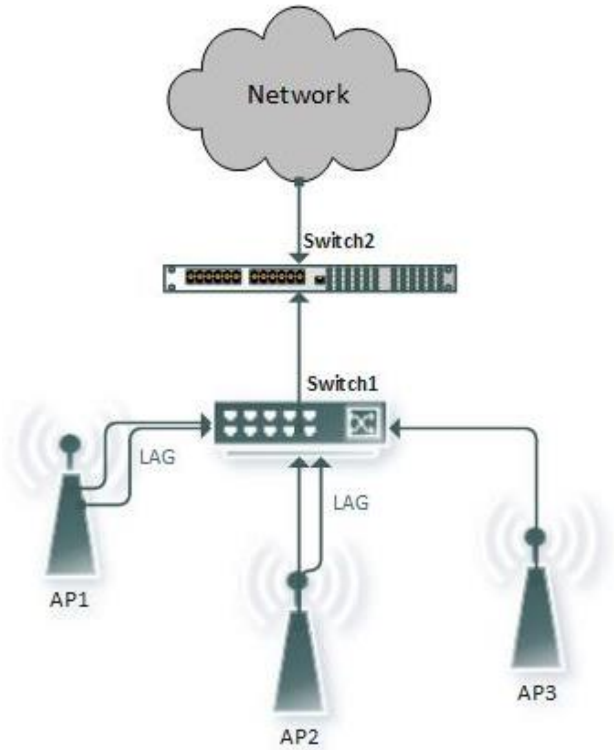
استفاده از AP در محیط های با ترافیک سنگین (heavy traffic) و تعداد Client بالا:

در اینچنین مواقع که حجم ترافیک زیاد است، به احتمال زیاد، استفاده از تنها یک کابل شبکه، جهت اتصال AP به DS، با مشکل مواجه خواهد شد.

در این حالت، از AP اي استفاده مي كنيم كه استاندارد 802.11ac نوع Phase-2 را پشتيباني كند، چون تنها این مدل است که قادر به پیاده سازی این قابلیت خواهد بود؛ و این مدل AP ها، معمولن گرانقیمت نیز می باشند.

پس درگاه AUX روی AP را نیز به Switch شبکه ی DS متصل کرده و سپس هردو اتصال را، با یکدیگر EtherChannel کنیم.

نکته: معمولاً چندین AP، به یک Switch1 متصل می شوند، و این Switch1 به یک Switch2 متصل است.



به جهت redundancy و امنیت اتصال میان AP و Switch1، بطورمثال، Link میان دو AP با Switch1 را، EtherChannel می کنیم؛ که به آن LAG (Link Aggregation Group) نیز گفته می شود.

نکته: ارتباط میان هریک از AP ها با Switch ای که به آن متصل است، در حالت Trunk خواهد بود.
چرا که یک AP می تواند چندین SSID، با ویژگی ها و دسترسی های متفاوت از هم را، منتشر کند، که درحقیقت هر SSID، فقط به شبکه ی یکی از VLAN ها متصل می باشد.

نکته: جهت راه اندازی LAG میان AP و Switch، لازم است که AP را، بر روی حالت Local Mode تنظیم کنیم (و نه Stand alone)

نکته: این LAG را می توانیم در یکی از حالت های LACP و یا Static mode تنظیم کنیم، چون AP ها، مدل PagP را نمی شناسند!

نکته: قبل از اتصال کامل و راه اندازی ارتباط AP با Switch، باید ابتدا در WLC نوع اتصال AP ها با Switch ها تنظیم شده باشند.

نکته: درصورتی که AP از نوع CISCO باشد، لازم است که Switch نیز، CISCO باشد.

Monitoring:

- **یکی از فعالیت های AP ها، نظارت بر محیط است.**
- **می دانیم که AP ها در یکی از کانال های باند فرکانسی 2.4 و یا 5 گیگاهرتز تنظیم و راه اندازی می شوند.**
- **جدا از اینکه یک AP بطورمداوم، در حال نظارت کانال خودش کار می کند، همچنین 0.2 درصد از زمان فعالیتش را، صرف اجرای عملیات**
- **Scan و نظارت بر کانال های دیگری که در محدوده ی باند فرکانسی خودش هستند، می کند، که به آن** Off-Channel Scanning **گفته می شود.**
- **این رفتار، به جهت بررسی این است که آیا AP دیگری در آن نزدیکی وجود دارد که SSID شبکه را منتشر کند؟!**
- **پس در روند این monitoring، در صورت مشاهده ی یک AP غریبه یا یک نفوذ ناشناس، آن را به WLC گزارش می دهد.**

➢ CAPWAP :

درحقیقت وقتی در شبکه ای از LAP و WLC استفاده می کنیم، یک ارتباط نرم افزاریِ تونل مانند، میان تک تک LAP ها با WLC، به شکل دایمی، برقرار می شود، که CAPWAP Tunnel نامیده می شود.

این CAPWAP Tunnel توسط پروتکلی به نام CAPWAP (Control And Provisioning of Wireless Access Points) ایجاد و مدیریت می شود.

- **WLC پیکربندی ها را توسط CAPWAP به همه ی AP ها، ابلاغ می کند.**
- **میان LAP ها و WLC می تواند یک یا چند Switch وجود داشته باشد، اما بالاخره باید LAP ها با WLC در یک شبکه باشند، که بتوانند همدیگر را Ping کنند.**

درحقیقت، CAPWAP شامل دو مسیر یا Tunnel خواهد بود:

- **CAPWAP Management and Control:**
  - ✓ از آنجایی که اطلاعات احراز هویت و پیکربندی و مدیریتی را ارسال و دریافت می کند، پس به شکل رمزنگاری شده (encrypted) کار می کند.
  - ✓ این encryption، توسط <u>پروتکل DTLS</u> و <u>استاندارد X.509</u> کار می کند.
  - ✓ Certificate ای که این رمزنگاری را تکمیل می کند، به شکل یک PKI است که از قبل بر روی دستگاه ها نصب شده است. (Pre-Installed)

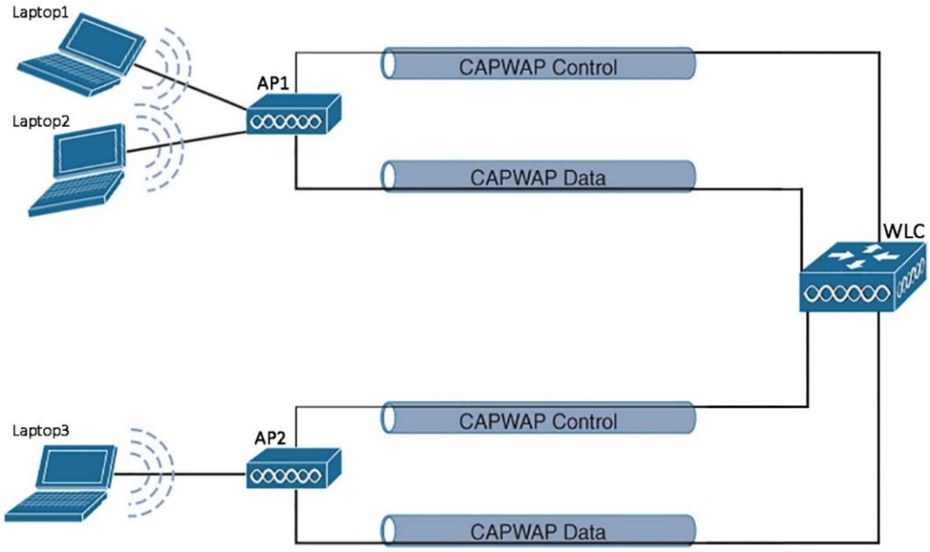
- **CAPWAP Data:**
  - ✓ تمام Data های Client ها، حتی Client هایی که به یک AP وصل هستند، از طریق این Tunnel جابجا می شوند.
  - ✓ این Tunnel به شکل پیشفرض، رمزنگاری نشده است، که می توان encryption را توسط <u>پروتکل DTLS</u> بر روی آن فعال کرد.

- ✓ **هردوی این Tunnel ها، از جنس UDP هستند.**
- ✓ **شماره Port هایی که برای هریک از این Tunnel استفاده می شوند، متفاوت و ثابت هستند:**

	CAPWAP Management and Control	CAPWAP Data
	U D P	
Port number	5246	5247

مثال؛ برطبق شکل زیر:

- ➢ **وقتی Laptop1 داده ای را به Laptop2 ارسال کند، ابتدا AP1، آن داده را از طریق CAPWAP Data به WLC ارسال کرده و WLC پس از بررسی، آن را توسط همان CAPWAP Data، به AP1 برمی گرداند و AP1 آن را به Laptop2 می فرستد.**
- ➢ **زمانی که Laptop1 داده ای را به Laptop3 ارسال کند، ابتدا AP1، آن داده را از طریق CAPWAP Data به WLC ارسال کرده و WLC پس از بررسی، آن را توسط CAPWAP Data ای که میان او و AP2 است، به AP2 ارسال می کند و AP2 آن را به Laptop3 می فرستد.**



پس با توجه به این عملیات رفت و برگشتی (round trip) **میان AP و WLC، لازم است که فاصله ی میان هر AP تا WLC آنقدر زیاد نباشد که زمان موردنیاز برای رسیدن بسته به مقصد، بیش از 100 ms شود.**
درحقیقت جایگاه فیزیکی WLC، باید جایی باشد که همه ی AP ها نزدیکترین فاصله ی ممکن را به آن داشته باشند.

نکته: اگر بیشتر تعاملات داده ای Client ها با Server است، و قرار بر تعامل زیاد داده ای میان خود Client ها با یکدیگر نباشد، پس بهترین مکان جهت نصب و راه اندازی WLC، در کنار Server هاست.

FlexConnect:

در شبکه های چند شعبه ای که WAN محسوب می شوند، و WLC در یکی از شعبه ها نصب و برقرار بوده و AP های هر شعبه برای برقراری هرارتباطی از سمت Client ها (حتی Client های local) **ابتدا باید Data ها یا درخواست ها را توسط تونل CAPWAP و در محیط WAN به WLC ارسال کنند، این روش کُند و ناایمن است، چون در صورت قطع شدن کانال WAN، به سادگی، AP ها هیچ کاری از دست شان برنخواهد آمد، AP ها بدون WLC عملن بی کاربرد خواهند بود.**
که در اینگونه شبکه های WAN، راهکار این است که برای هر شعبه، یک WLC تهیه و راه اندازی کنیم، که البته راهکار گرانی خواهد بود!

پس CISCO راهکار جدیدی ارایه کرد، به این صورت که یک قابلیت در تنظیمات AP ها و WLC اضافه شده است، به نام FlexConnect، که در صورت فعال کردن آن هم بر روی WLC و هم بر روی AP، دیگر جهت تبادل داده میان Client های local، نیازی به ارسال Data ها به سمت WLC ارسال نخواهند شد، بلکه خود AP، این جابجایی را منتقل می کند.

از دیگر قابلیت های حالت FlexConnect:

- درصورت قطع شدن CAPWAP Tunnel میان AP و WLC، مثل حالات قبل، AP بی کاربرد نخواهد شد، بلکه خودش به سادگی، وارد حالت **Stand alone** شده و ارتباطات local را همچنان منتقل و هدایت می کند.

پس قابلیت FlexConnect، دو حالت دارد:

- **Connected mode**: وقتی که ارتباط LAP با WLC برقرار باشد.
- **Standalone mode**: وقتی که ارتباط LAP با WLC قطع باشد.

درحقیقت هنگام خرید WLC یا AP، باید دقت داشت که این قابلیت را پشتیبانی کند.

Converged Wireless network:

درحقیقت، در Switch های نسل جدید، قابلیت WLC به شکل یک گزینه ی جدید، درون خود آن، تعبیه شده است.
از مزایای این معماری، شباهت آن با قابلیت FlexConnect است، که دیگر جهت تبادل داده میان WiFi Client ها و یا میان AP ها، ، نیازی به ارسال Data ها به سمت WLC اصلی در رده های بالاتر نخواهد بود، بلکه خود Switch ای که AP ها به آن متصل هستند، این جابجایی را منتقل می کند.
نکته: خود Switch باید این قابلیت را پشتیبانی کند.
پس در این معماری، WLC حتی تا لایه های Distribution یا Access Layer پایین می آید.

➢ Radio Type :

درحقیقت به نوع ارتباط بی سیم که دستگاه ها تحت آن، با قدرت و توان های خاص، با یکدیگر ارتباط برقرار می کنند، **Radio type** یا **استاندارد WiFi** گفته می شود. مشخصه های مهم استانداردهای ارتباط توسط دستگاه های **WiFi Certified**:

Standard name	Frequncy band	Max Data rate (Speed)	Note
802.11b	2.4 GHz	11 Mbps	
802.11g	2.4 GHz	54 Mbps	
802.11a	5 GHz	54 Mbps	
802.11n	2.4 GHz and 5 GHz	600 Mbps	Called WiFi 4
802.11ac	5 GHz	1.3 Gbps ~ 2.3 Gbps	Called WiFi 5
802.11ax	2.4 GHz and 5 GHz	9.6 Gbps	Called WiFi 6

❖ اگر دو دستگاه در **یک باند فرکانسی یکسان** با هم مرتبط باشند، کافی خواهد بود و می توانند باهم کار کنند، و اینکه سرعت های متفاوت داشته باشند، مهم نیست.

❖ درحقیقت، این قطعه ی **Transceiver** موجود بر روی هر دستگاه است که یکی از استانداردهای مختلف **802.11** را پشتیبانی می کند.

❖ **Transceiver**، اولین قطعه ای روی هر دستگاه (Laptop، Smartphone و ...) است که آنتن، به آن متصل خواهد بود.
مثلاً وقتی یک دستگاه، چند استاندارد **802.11** را پشتیبانی می کند، به این معنی است که به تعداد آن استانداردها، دارای قطعه ی **Transceiver** می باشد.

❖ فناوری **MIMO** یا **multipleInput-multipleOutput** در سیستم های **wifi** جهت **کاهش تاخیر** و **تقویت سیگنالهای دریافتی** استفاده می شود، که در استاندارد **802.11n** بکار گرفته می شود.

❖ **Bluetooth** تکنولوژی انتقال داده توسط امواج کوتاه برد رادیویی (الکترومغناطیسی) است.
- حداکثر تا **100** متر فاصله قابلیت انتقال دارد.
- فرکانس مورد استفاده برای آن در باند **2.4 GHz** تا **2.48 GHz** می باشد.

➢ Network Type :

سه حالت برای راه اندازی یک شبکه ی Wireless Lan وجود دارد، که در حالت کلی، نوع شبکه، با این حالات شناخته می شود:

▪ **Ad Hoc mode :**

- نیاز به یک دستگاه مرکزی مثل Access Point نیست.
- کامپیوترها توسط کارت شبکه ی Wireless ای که دارند، به شکل مستقیم با هم ارتباط برقرار می کنند.
- ارزان تر و راحت تر است.
- ناامن تر است!

▪ **Infrastructure mode :**

- شامل یک دستگاه مرکزی به نام Access Point می باشد که بصورت بی سیم با Node های شبکه در تماس است.

▪ **Mesh mode :**

- با توجه به اینکه، همه ی AP ها بالاخره نیاز به یک اتصال wired جهت Uplink دارند، زمانی که امکان کابلکشی وجود نداشته باشد، مجبور خواهیم بود، حداقل uplink یکی از AP ها را به شکل wired متصل کنیم، اما uplink هریک از AP های دیگر را به شکل wireless به نزدیکترین AP اش متصل خواهیم کرد.
- این حالت، ناامن و البته کُند است.
- بیشتر در محیط های outdoor کاربرد دارد.

➢ Wireless Lan Controller (WLC):

فرض کنید در یک شرکت، بیش از دو عدد Access Point داشته باشیم.
پس اتصال به تک تک آنها جهت تنظیم و راه اندازی، و یا جهت به روزرسانی های دوره ای، زمانگیر و طاقتفرسا خواهد بود.
پس با تهیه ی یک WLC و اتصال همه ی AP ها به آن، همه ی تغییرات موردنظر را طوری بر روی WLC انجام می دهیم، که بر روی همه ی AP ها اعمال شوند.

بطورکلی، WLC به دو شکل وجود دارد:

- **Appliance**: یعنی WLC به شکل یک دستگاه فیزیکی است. (به جهت نیاز به منابع سخت افزاری، گران قیمت تر است.)
- **Cloud-based**: یعنی WLC به شکل یک نرم افزار است؛ و دو حالت دارد:
  - **WLC on a Private cloud: نرم افزار WLC را بر روی یک Server راه اندازی می کنیم.**
  - **WLC on a Public cloud: بستر مدیریت WLC بر روی یک سرویس Cloud عمومی** (مثل Amazon) **راه اندازی می شود.**

نکته: درحقیقت در این روش، داده های Client ها به سمت Public Cloud نمی روند، تنها چیزی که میان Cloud و شبکه مبادله می شود، Control plane و management plane می باشد.

برخی مشخصه های مهم WLC ها:

- **تعداد Client های قابل پشتیبانی: یک WLC می تواند 2000 و یا حتی تا بیشتر Client را جهت مدیریت اتصال به شبکه، پشتیبانی کند.**
- **تعداد و نوع Uplink ها: یک WLC می تواند دو Uplink Interface داشته باشد که 1Gbps باشند، و یا چهار Interface که 10Gbps باشند.**

درگاه های عمومی یک WLC:

- Console Port: جهت انجام اولین اتصال به یک WLC و پیکربندیِ آن نیز، یک کامپیوتر را توسط کابل Console به Console Port آن متصل می کنیم.
- Service Port: پس از پیکربندی و راه اندازی WLC و احتمالن اتصال آن به AP ها، جهت اتصال خود WLC به شبکه، از این درگاه استفاده می کنیم، که باید یک IP در محدوده ی آدرسِ شبکه مان، به آن اختصاص دهیم، و به این صورت می توان توسط SSH و Telnet هم به آن متصل شد.
- Redundancy Port:

درحقیقت، درصورت از کار افتادن WLC، ارتباط و Data ها و تنظیم های همه ی AP ها، از بین خواهند رفت.
پس لازم است که حداقل از یک WLC زاپاس (Redundant) هم استفاده کنیم.
این redundant WLC به طورمستقیم به خود WLC اصلی متصل شده و تنظیمات و داده هایشان را مدام با هم همگام سازی می کنند.
پس WLC ها، از طریق درگاه Redundancy به یکدیگر وصل می شوند، که فقط یکی از آنها به شکل فعال کار خواهد کرد.

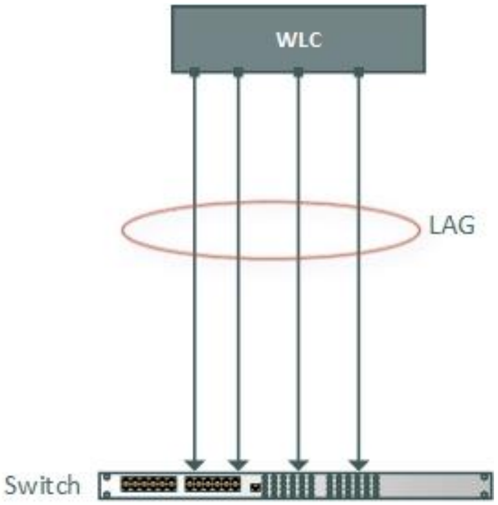
- Ethernet Port: هر WLC، همچنین دارای چندین Ethernet Port می باشد که توسط آنها، AP ها به آن متصل می شوند، اما در عمل، Switch ای که به همه ی AP ها متصل است، به این درگاه های WLC، وصل می شود.

نکته: بطورمعمول، هر اتصال WLC با Switch را بر روی Trunk قرار می دهیم.

درحقیقت، به جهت redundancy و امنیت این اتصال میان WLC و Switch، این Link، توسط چند اتصال برقرار می شود؛ و سپس همه ی آن Link ها، با یکدیگر یک EtherChannel تشکیل می دهند، که به آن LAG (Link Aggregation Group) **گفته می شود.**

نکته: حالت این LAG را بر روی Static EtherChannel تنظیم می کنیم، که mode را ON تنظیم می کنیم، چون **WLC**، دو مدل **PagP** و **LACP** را نمی شناسد!

نکته: در تنظیمات EtherChannel بر روی Switch، لازم است که Load balancing را بر روی layer 4 قرار دهیم. (بهترین حالت ممکن)



- <u>Virtual Interface</u>:
  - ✓ درحقیقت، برای AP هایی که به WLC متصل می شوند، یک پورت مجازی بر روی WLC موجود خواهد بود، که به آن AP Manager گفته می شود و ارتباطات AP ها، بر اساس آن پورت مجازی کنترل می شوند.
  - ✓ اگر میان WLC و Switch بیش از یک Link موجود باشد، به ازای هر Link، یک AP Manager در WLC ایجاد خواهد شد، که به یک یا تعدادی از AP های شبکه اختصاص داده خواهد شد؛ در این حالت، اگر یکی از Link های میان WLC و Switch قطع شود، ارتباط همه ی آن AP هایی که تحت آن Link، یک AP Manger دریافت کرده بودند، قطع شده، و AP ها یکبار خاموش و روشن شده و اینبار به یکی دیگر از AP Manger های موجود متصل می شوند.
  - ✓ آدرس IP آن پورت مجازی و آدرس IP مربوط به AP هایی که به آن متصل هستند، باید در یک شبکه باشند.
  - ✓ اگر توسط Link های میان WLC و Switch، یک LAG ایجاد کرده باشیم، پس فقط یک AP Manager بر روی WLC ایجاد خواهد شد که در صورت قطع شدن یکی از Link ها، ارتباط AP ها همچنان برقرار خواهد بود.

نکته: ارتباط میان WLC با SW، بطورمعمول بر روی Trunk خواهد بود؛ که درنتیجه ارتباط میان SW های میان WLC تا AP نیز از نوع Trunk خواهد بود.

درحقیقت برای خرید و تهیه ی WLC، با گزینه های زیر مواجه هستیم:

- **Physical Controller:**
  - این WLC ها، از لحاظ <u>میزان throughput</u> و <u>تعداد AP ها</u> و <u>تعداد Client</u> هایی که می توانند پشتیبانی کنند، دسته بندی می شوند.
  - نیاز به تهیه ی یک License برای آن می باشد.
- **Cloud Controller:**
  - دردسرهای پیکربندی و نصب و راه اندازی و به روزرسانی، حذف می شوند، هیچ محدودیتی برای تعداد AP و Client ندارد.
  - در ابتدا باید یک Subscription در سایت Cloud مربوطه، خریداری نمود.
- **: Embedded wireless**
  - گاهی WLC به شکل یک قطعه (ماژول)، درون Switch تعبیه شده است.
  - راهکاری کم هزینه بوده و به سادگی قابل راه اندازی است.
- **Mobility Express:**
  - قابلیت WLC، بر رو بعضی AP ها تعبیه شده است. پس یکی از AP ها را به عنوان WLC تنظیم می کنیم.
  - AP ای که نقش WLC را می گیرد، قادر به مدیریت تا 100 عدد AP دیگر خواهد بود.
  - کم هزینه ترین راهکار است.
  - پس یک AP، بقیه ی AP ها نظارت و مدیریت می کند.
  - هیچ نیازی به تهیه ی License نخواهد بود.
  - معادل این مدل AP ها، برای شرکت Aruba را با عبارت **Aruba Instant** مشخص می کنند.

➢ Access Point Modes :

درحقیقت AP ها در mode های مختلفی کار می کنند و تصمیم گیری اینکه در چه mode ای باشند، برعهده ی WLC خواهد بود. گزینه هایی که بسته به mode، تغییر می کنند:

- ➢ **وابسته به WLC کار کند یا خیر؟** (If an AP associated with a WLC)
- ➢ **آیا AP به Client ها سرویس می کند یا خیر؟**
- ➢ **چگونگی دریافت Wifi frame های Client ها در AP.**
- ➢ **چگونگی ثبت و گزارش دادن وضعیت امواج رادیویی**

Local mode:

- **این حالت، حالت پیشفرض برای LAP ها خواهد بود.**
- **همه ی Data ها و اطلاعات مدیریتی و کنترلی، توسط CAPWAP Tunnel ارسال و دریافت می شوند.**
- **اگر CAPWAP Tunnel قطع شود، ارتباط با همه ی Client هایی که به AP وصل بوده اند، قطع می شود.**

Bridged mode:

- **از این حالت، به ندرت استفاده می شود.**
- **Access Point ای که در این حالت استفاده می شود، باید یک Ethernet Port داشته باشد.**
- **بر طبق این حالت، یک Autonomous AP می تواند به شبکه ای که یک LAP منتشر می کند، متصل شود.**

بطورمثال شبکه ای داریم که در آن، AP ها توسط WLC مدیریت می شوند، پس همه ی AP ها، LAP هستند.
حال در مکانی در محیط شبکه، یک Printer که حداقل یک درگاه شبکه دارد، اما اصلن ارتباط WiFi را پشتیبانی نمی کند، فاصله ی زیاد یا پیچیده ای وجود دارد، تا این Printer، توسط کابل، به شبکه متصل شود.
پس یک AP را به درگاه شبکه ی Printer وصل کرده و آن را روی حالت Bridged و طوری تنظیم می کنیم که امواج شبکه را از نزدیکترین LAP دریافت کند.

Repeater mode:

- **از این حالت، به ندرت استفاده می شود.**
- **از این mode برای گسترده تر کردن شبکه ی Wireless استفاده می شود. به این ترتیب که یک AP، سیگنال WiFi را دریافت و سپس تقویت می کند، و برای AP بعدی ارسال می کند.**
- **پس در این Mode هر دستگاه هم می تواند Data را دریافت و هم آن را ارسال کند.**
- **از این حالت، بیشتر در فضاهای بزرگ استفاده می شود.**

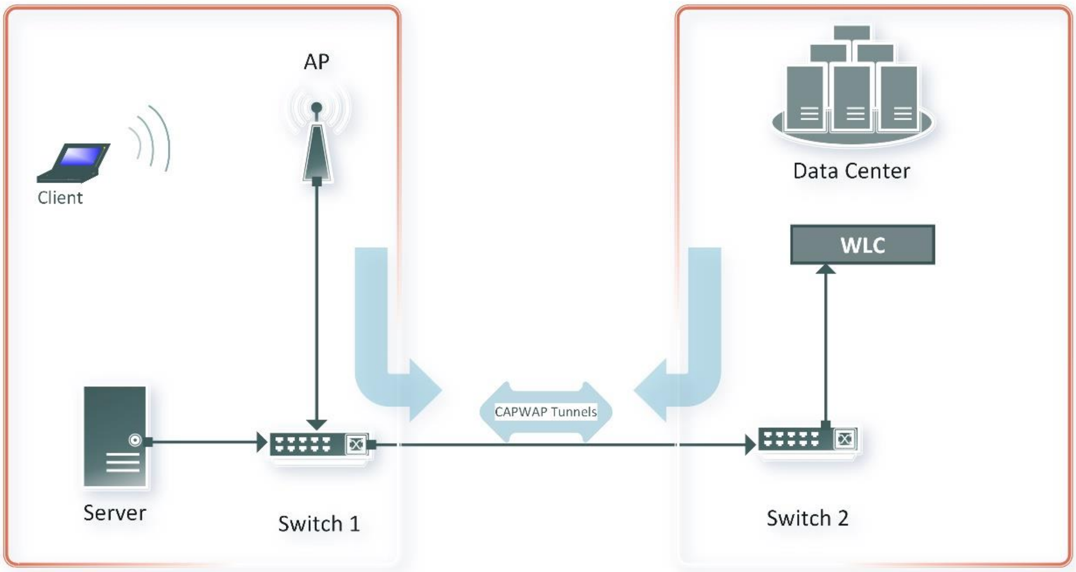
:(H-REAP) FlexConnect mode

این **mode** با نام Hybrid Remote Edge Access Point (**H-REAP**) هم شناخته می شود.

شبکه ی زیر را درنظر بگیرید، که شامل دو ساختمان است، یکی شبکه ی اصلی و دیگری **Data Center** شبکه.

WLC در ساختمان **Data Center** و **Server** در ساختمان شبکه ی اصلی قرار دارد.

پس در هربار درخواست ارتباط با **Server**، نیاز است که ارتباط میان **Server** و **Client**، توسط **CAPWAP Tunnel** که یک مسیر رفت و برگشتی طولانی است، بررسی و برقرار شود.



پس در صورتی که هم **AP** و هم **WLC**، حالت **FlexConnect** را پشتیبانی کنند، اگر **mode** آنها را بر روی **FlexConnect** قرار دهیم، دیگر در هربار درخواست **Client** جهت ارتباط با **Server**، نیازی به ارسال و دریافت **Packet** ها بر روی **CAPWAP Tunnel** نخواهد بود، بلکه **AP** بسته ها را مستقیم به **Server** هدایت کرده و پاسخ را دریافت و به **Client** ارسال می کند.

درحقیقت، در این حالت، نیاز است که دو **SSID** در شبکه تعریف کرده باشیم، که یکی مربوط به خود ساختمان مربوط به **SW1** باشد، و دیگری مربوط به تمام شبکه ی موجود باشد. سپس تعیین می کنیم که ترافیک موجود در **SSID** اول، در حالت **FlexConnect** کار کند که نیازی به ارسال ترافیک به **WLC** جهت تایید کردن و پاسخ دادن به درخواست ها نباشد.

:Monitor mode

- **Client** ها قادر به متصل شدن به **AP** ای که روی این حالت قرار می گیرد، نیستند.
- در این حالت، **AP** ، هر **12** ثانیه، هریک از **Channel** ها را **Scan** کرده و دستگاه هایی که بطورغیرمجاز به شبکه متصل شده اند و یا **AP** هایی که کانال های غیرهماهنگ شده را سر از خود، منتشر و تبلیغ می کنند را شناسایی و اطلاعات به دست آمده را به **WLC** ارسال می کند.

روش استفاده از Monitor mode:

فرض کنید در شبکه ای که داریم، قرار است که هر **30** متر یا هر **50** متر، یک **AP** نصب و راه اندازی کنیم.

منطقی خواهد بود که در میان هر دو **AP** ، یک **AP** در حالت **monitor** قرار دهیم؛ تا این **AP monitor mode**، تمامی شرایط و ارتباطات مربوط به دو **AP** کناری اش را بررسی و به **WLC** ارسال کند.

:Sniffer mode

- این حالت، مشابه **monitor mode** می باشد، با این تفاوت که برخلاف **monitor mode** که همه ی کانال های **2.4 Ghz** و **5Ghz** بررسی و **scan** می شدند، در این **mode**، آن را طوری تنظیم می کنیم که فقط یک کانال خاص موردنظر را **scan** کند.
- این تنظیم را بر روی **WLC** انجام می دهیم، طوری که **AP** موردنظر را بر روی **sniffer mode** قرار دهد، و کانال موردنظر برای آن، بطورمثال باند **5Ghz** و کانال **40** باشد.

در ادامه همه ی ترافیک موجود در کانال **40** مربوط به **AP** های پیرامون **sniffer mode AP** مورد نظر، به سمت **WLC** ارسال خواهند شد، که این قابلیت نیز در **monitor mode** وجود ندارد.

از آنجاییکه در این **mode**، همه ی ترافیک موردنظر، بطورکامل توسط **sniffer mode AP** دریافت و به سمت **WLC** ارسال می شود:

- اولن: عملکرد این **AP** مشابه یک جاسوس خواهد بود.
- دومن: می توانیم طوری تنظیم کنیم که **WLC** همه ی ترافیک دریافتی از **sniffer mode AP** را به سمت یک **Server** هدایت کند؛ که در ادامه در این **Server** این ترافیک دریافتی، توسط یک نرم افزار، تجزیه و تحلیل شود.

  نرم افزارهای رایج در این زمینه:

  - Wireshark
  - Omnipeek
  - Airopeak
  - AirMagnet

این نرم افزارها، ورودی را توسط **UDP Port** (source port: 5555 / Dest. Port: 5000) در WLC دریافت می کنند.

:Sensor mode

در شبکه های بزرگ که تعداد **Wifi Client** ها بسیار بالاست و در صورت بروز هرگونه مشکل برای هریک از کاربرها در هر نقطه از شبکه، نمی توان به سادگی شرایط او را از راه دور بررسی و عیبیابی کرد، و یا به صرفه نخواهد بود که مدیر شبکه مسافت فیزیکی را طی کند تا به آن نقطه ی موردنظر رفته و شرایط را بررسی کند، در کنار هر چند **AP** در شبکه، یک **AP** دیگر قرار می دهیم و در حالت **Sensor mode** تنظیم می کنیم.

- این **AP**، مشابه یک **Wifi Client** به **AP** های دیگر متصل می شود، و از سوی دیگر، شرایط و مشخصات ترافیک مربوط به آن **AP** ها را به سمت **WLC** ارسال می کند.
- مزیت مهم این **mode** این است که حتی قبل از اینکه **Client** ها متوجه مشکل شوند، **Admin** متوجه مشکل خواهد شد.
- نکته مهم در مورد **sensor mode AP** این است که در حقیقت:
  - **DNA Center** شبکه، دارای تعداد زیادی **Profile** و **Template** های تست و تجزیه و تحلیل شبکه است.
  - **DNA Center**، این **Profile** ها و **Template** ها را بر روی **WLC** شبکه **load** می کند.
  - **WLC** هم این الگوهای بررسی شبکه را بر روی **sensor mode AP** ارسال و **load** می کند.
  - **sensor mode AP** هم تست کیفیت شبکه را بر اساس همین **Profile** و **Template** ها انجام می دهد و نتیجه ای که به دست می آورد را بطورمستقیم به سوی **DNA Center** ارسال می کند، بدون اینکه **WLC** را از آن نتیجه مطلع کند.
  - در پایان **DNA Center**، نمودارهای کیفی و کمی شبکه را بر اساس نتایج بدست آمده از **Sensor mode AP** نمایش می دهد.

:Mesh mode

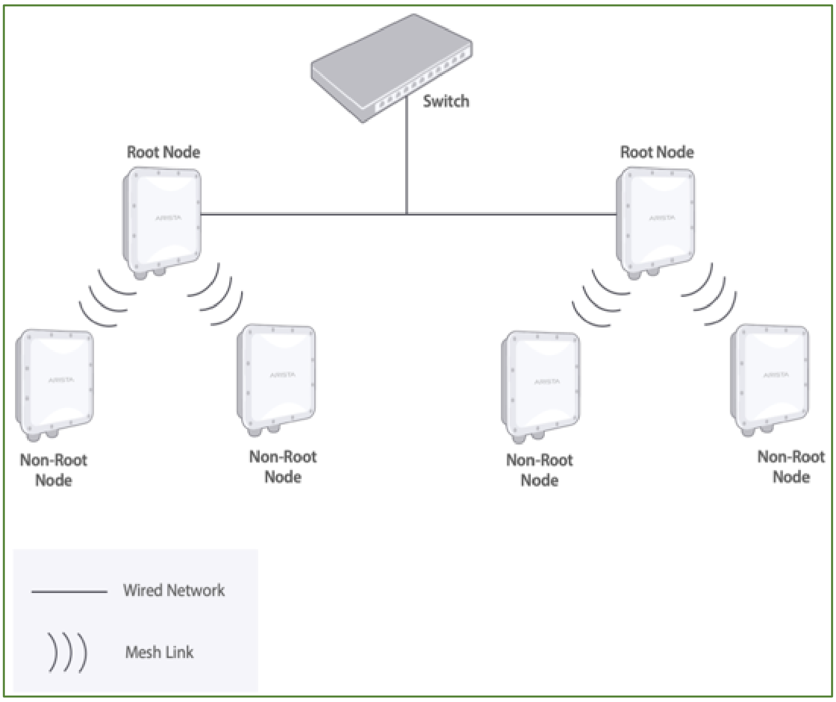
گاهی در محیط های بزرگ، و یا در محیط های مرتفع، امکان اتصال **AP** یا **AP** ها به شکل کابلی به **Switch** شبکه، امکان پذیر یا بصرفه نیست.

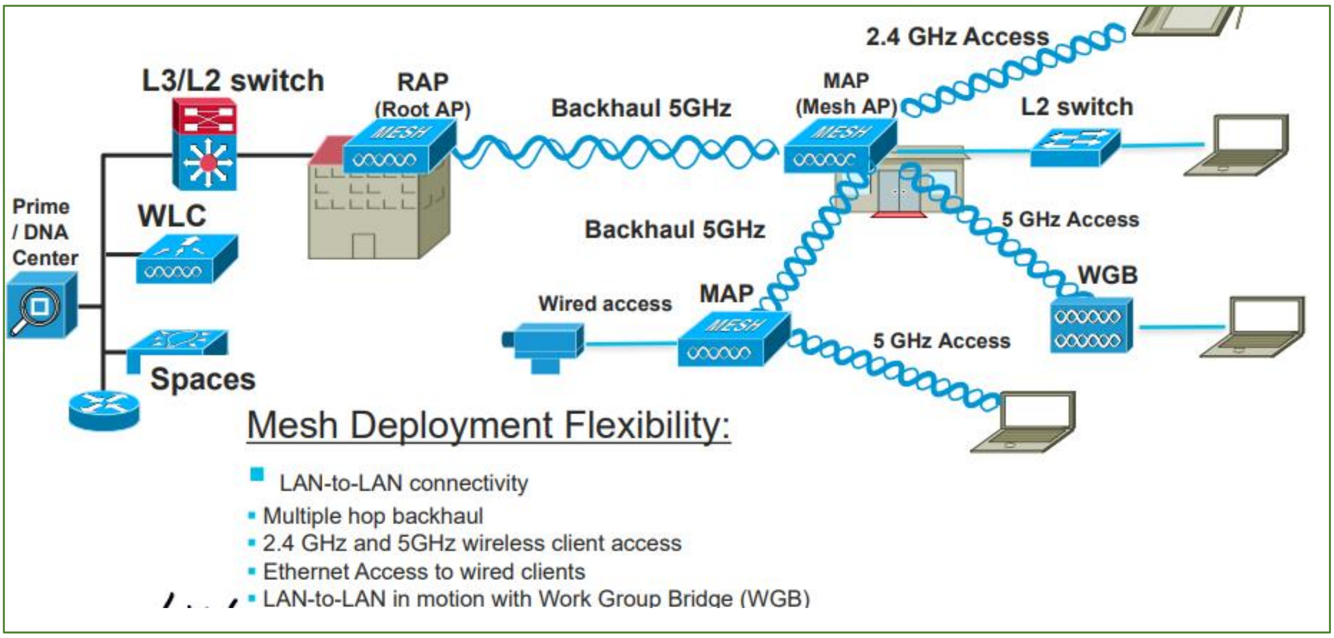
در این حالت، کافی ست **AP** موردنظر را به شکل بی سیم، و به کمک **mesh mode**، به نزدیکترین **AP** متصل کنیم.

اگر نزدیکترین **AP** هم ارتباط کابلی با شبکه نداشت، آن را نیز توسط **mesh mode** و به شکل بی سیم به نزدیکترین **AP** متصل می کنیم.

- به **AP** هایی که در حالت **mesh mode** هستند **MAP** (mesh AP) گفته می شود.
- و بالاخره به اولین **AP** ای که توسط کابل، به **Switch** شبکه متصل است، **RAP** (Route AP) گفته می شود.

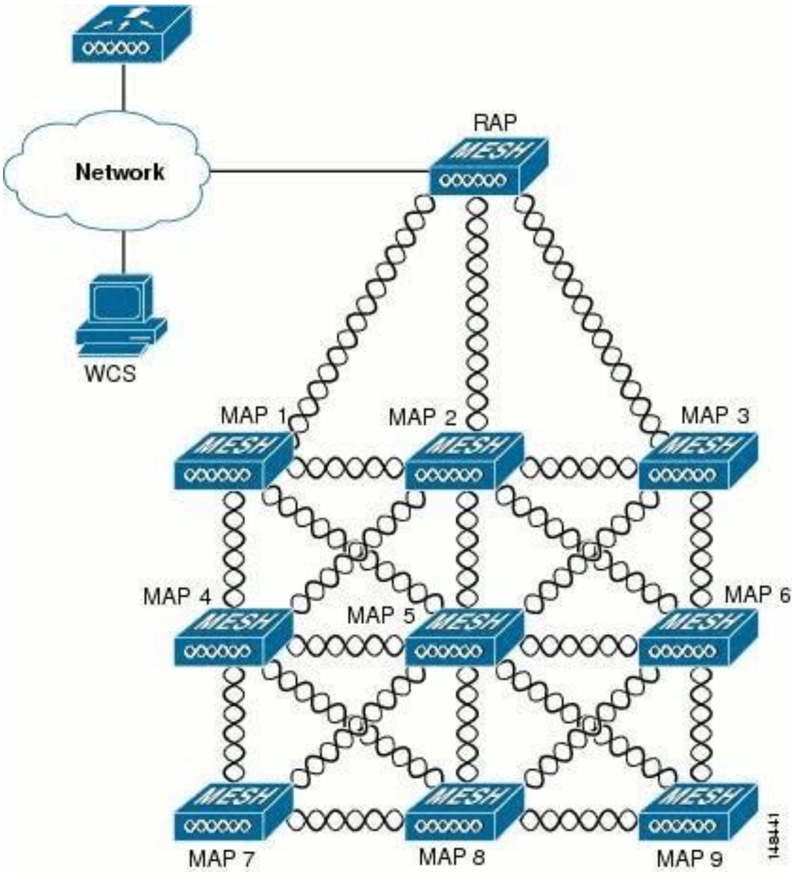
- درحقیقت همه ی MAP ها به شکل wireless با هم در ارتباط هستند.
- پس در هنگام پیکربندی AP ها، لازم است که نوع MAP یا RAP آنها مشخص کنیم.





- هریک از Mesh AP ها، همچنان قادر خواهند بود در mode های دیگر نیز (Monitor ،Sniffer ،Sensor) کار کنند.

- ارتباط میان **MAP** ها با **RAP**، توسط یک پروتکل به نام **AWPP** (Adaptive Wireless Path Protocol) انجام می شود. ضرورت این پروتکل به این جهت است که زمانی که **MAP** های زیادی وجود داشته باشند، لازم است که ترافیک هریک از **MAP** ها، سریع ترین و کوتاه ترین مسیر را جهت رسیدن به **RAP**، هدایت شود.



- بطوراساسی، بازدهی **Mesh AP** ها پایین و ضعیف خواهد بود؛ چرا که وقتی یک **MAP** درحال تبادل ترافیک با یک **Client** در یک کانال از باند **2.4 Ghz** است، نمی تواند در همان کانال و همزمان، با **MAP** دیگر در همان کانال تبادل ترافیک کند. پس برای رفع این مشکل، ارتباط میان **MAP ها با Client ها** در فرکانس **2.4GHz** و ارتباط میان **MAP ها با یکدیگر**، در فرکانس **5GHz** می باشد.

WiFi Security :

اصل اول این است که تامین امنیت در شبکه های wireless، خیلی مهم تر و خیلی دشوارتر از در شبکه های wired می باشد.

نگرانی Wifi Admin ها:

1. **به شبکه ی سازمان، تنها authorized Clients** (کاربرهای احراز هویت شده) **اجازه ی دسترسی داشته باشند.**
   یعنی Client ای که به یک شکلی، authenticate شده باشد.
2. **برای authorized Clients ها، تنها authorized resources** (داده های مجازِ مربوطه) **قابل دسترسی باشند.**
3. **تعیین محدودیت برای تعداد Client های قابل سرویس دهی برای هر AP.**
4. **تشخیص rogue AP های احتمالی.**
   نکته: rogue AP، یک unauthorized AP است که در منطقه ای از سازمان، یک SSID مربوط به خود را که یک unauthorized SSID خواهد بود را در شبکه تبلیغ می کند.

اقدامات لازم جهت رفع نگرانی Wifi Admin ها:

1. **رمزنگاری** (encrypt) **کردن داده هایی که با AP مبادله می کند و حفظ امنیت و محرمانگی آنها.** (Data confidentiality)
   نکته: درحقیقت، Authenticating هیچ ربطی به encrypting ندارد؛ طوری که ارتباط یک authenticated Client می تواند **un**encrypted باشد.
2. **یکپارچگی و عدم دستکاری و تغییر داده هایی که ارسال یا دریافت می شوند.** (Data Integrity)

بر اساس نگرانی های بالا، می توان سه گزینه ی اصلی Wifi Security را به شکل زیر خلاصه کرد؛ که اینها را با اختصار CIA می شناسند:

- **A**uthentication
- **C**onfidentiality
- **I**ntegrity

➢ Association:

برقرار شدن ارتباط میان یک Client با یک AP، با نام Association (پیوند / اتصال) شناخته می شود، که شامل چهار مرحله یا فاز است:

1- **Discovery:**

در این مرحله Client، توسط AP موجود در شبکه، WLAN را شناسایی می کند.

این مرحله به دو شکل قابل انجام است:

روش اول:

- به محض اینکه یک wifi client روشن می شود، شروع به ارسال بسته های **Probe request** تحت سیگنال های wifi در شبکه می کند، که نوعی جستجوی شبکه ی wireless می باشد.
- AP شبکه، پس از دریافت .Prob. Req ، با ارسال یک بسته به نام **Probe response** به سوی آن Client، اعلام حضور و خودش را معرفی می کند. این بسته ی پاسخ، حاوی **SSID** و **Frequency band** و **Channel number** و نیاز یا عدم نیاز به **passphrase** و ... می باشد.

روش دوم:

- در برخی شبکه ها، client ها، هیچ بسته ی .Prob. Req ای ارسال نمی کنند. پس منتظر بسته های تبلیغی از سوی AP ها می مانند.
- پس AP شبکه، با ارسال بسته ای به نام Beacon frame به تعداد 100 بار در ثانیه، خودش را در محیط، تبلیغ می کند.
- سپس Client با دریافت Beacon frame، به آن پاسخ خواهد داد، تا جایی که ارتباط آنها برقرار شود.

2- **Type of Authentication:**

در این مرحله، AP با ارسال یک بسته ی Beacon frame، کلیه ی مشخصه های احراز هویت را به Client ارسال می کند؛ و یا اگر که open authentication باشد، نیز آن را تحت همین بسته، اعلام می کند.

3- **Authentication Request/Response Frame:**

درصورتی که ارتباط با AP، بصورت .open Auth نباشد، در این مرحله:

- Client یک بسته به نام Authentication Request را به AP ارسال می کند.
- سپس AP در پاسخ، یک بسته ی Authentication Response به سوی Client ارسال می کند؛ که در این بسته ی پاسخ، یا اعلام می کند، که آماده و قادر به دریافت Passphrase می باشد، و یا اینکه درخواست Client را رد می کند.

4- **Association Request/Response Frame:**

- درصورتی که Passphrase (درصورت نیاز) با موفقیت ارسال و پذیرش شده باشد. حال در این مرحله، Client از AP می پرسد، آیا فضای موردنیاز برای او موجود است یا خیر.

نکته: می دانیم یک AP، با توجه به توانی که دارد، قادر به سرویس دهی به تعداد محدودی Client می باشد. پس Admin از قبل، این محدودیت را توسط WLC بر روی AP تعریف کرده است که تنها تعداد محدودی Client قابل سرویس دهی باشند.

- در صورت مثبت بودن پاسخ، AP یک Unique ID را به Response Frame ضمیمه و به سوی Client ارسال می کند؛ و سپس ارتباط برقرار می شود.

➢ Authentication :

برای جلوگیری از استفاده ی بی اجازه از شبکه ی Wifi از «احراز هویت» استفاده می شود.
وقتی که یک Client، سعی در اتصال به یک WiFi Profile دارد، چندین راه، جهت امن سازی فرآیند authentication برای او وجود دارد.
مفهوم ساده و مستقیم احراز هویت: تدارکِ یک شناسه و رمزعبور برای کاربر، جهت اتصال به شبکه.

بطورکلی دو نوع Authentication وجود دارد:

➢ User Authentication :

یکی از روش ها در این نوع از احراز هویت، Web Authentication است که Captive Portal هم نامیده می شود.
پس از Association، تازه یک صفحه ی Web باز می شود و باید یک User و password وارد کنیم.

➢ Device Authentication :

سه روش در این نوع از احراز هویت:

- **MAC address** filtering
- Assignment of **Certificate**
- **802.1x**

نکته: وقتی در یک wifi device، کادری که لیست wifi های موجود را نشان می دهد را باز می کنیم، یکی از مشخصه های همه ی Wifi ها، قسمت Security است، که اگر برای این گزینه، مقدار None درج شده باشد، به این معناست که آن Wifi، نیازی به Authenticating ندارد، یا Open Authentication است.

- **اگر دسترسی به wifi را باز گذاشته باشیم،** (open authentication باشد) **اما نگران دسترسی همسایه ها یا افراد خارج، به wifi نیز باشیم، بهترین راهکار، محدود کردن برد امواج wifi در درون خود ساختمان است، که با کاهش radio power level انجام می شود.**
- **برای اینکه دسترسی به wireless Router شبکه ی اداره را از خارج از ساختمان اداره هم تا جای ممکن برقرار کنیم، باید برد امواج wifi یا همان radio power level را افزایش دهیم.**

- **جهت افزایش امنیت شبکه ی wireless می توان در تنظیمات، SSID broadcast را disable کرد که در این صورت، در لیست شبکه های بی سیم موجود، نام آن را به شکل unnamed می بینیم که جهت اتصال به آن، کافی ست آن را انتخاب کرده و Password را وارد کنیم تا وصل شود.**

➢ Encryption:

درحقیقت الزامی در authenticating برای یک ارتباط encrypted وجود ندارد.
یعنی اتصال به یک SSID می تواند همزمان هم Encrypted **و هم** Open Authentication **باشد.**
نکته: در لیست Wifi های موجود در محیط، علامت قفل که در مقابل برخی SSID ها قرار می گیرد، نشانه ی encrypted بودن آن است؛ و ربطی به Authentication آن SSID ندارد.

- **شیوه های مختلفی برای رمزنگاری شبکه‌های WiFi وجود دارد که هریک، از الگوریتم ها و پروتکل های خاصی تشکیل شده اند.**
- **می دانیم که یک Packet علاوه بر اصل Data** (که Body نامیده می شود)**، حاوی بخش Header نیز می باشد؛ پس در طی عملیات encryption، تنها قسمت Body رمزنگاری می شود.**
- **همچنین بسته های مدیریتی** (Management packets) **که میان AP و Client مبادله می شوند نیز، رمزنگاری نمی شوند.**
- **درحقیقت Wifi encryption protocol ها، فقط بستر Wireless Packet ها را رمزنگاری می کنند، به این معنا که دامنه ی رمزنگاری آنها، end to end نیست! چرا که وقتی Packet ارسال شده از Client، در AP دریافت می شود، در همانجا decrypt می شود، که در صورتی که در بستر شبکه ی wired هیچ پروتکل رمزنگاری وجود نداشته باشد، Packet موردنظر، در ادامه ی مسیرش به سمت مقصد، به شکل clear text خواهد بود.**

- **خود Encryption، بخشی از Bandwidth را اشغال می کند، اما هیچ تفاوتی در تغییر در سرعت ارتباط نخواهد داشت.**
- **در زیر، پروتکل هایی که الگوریتم رمزنگاری مخصوص به خود را دارند، به ترتیبِ قدرت و امنیت لیست شده اند:**

- **پایگاه یا انجمنی وجود دارد به نام Wi-Fi Alliance که استانداردهای wireless قابل استفاده بر روی دستگاه های سیار را مدیریت می کند؛ و وقتی یک دستگاه، استانداردهای موردتایید این انجمن را دارا باشد، از خود این انجمن، یک تاییدیه به نام Wi-Fi CERTIFIED دریافت خواهد کرد.**

Wi Fi CERTIFIED

- **خود اتحادیه ی Wi-Fi Alliance، استانداردهایش را بر اساس، تنظیمات و پیکربندی هایی که در IEEE منتشر می شوند، ایجاد می کند.**

:WEP

- پروتکل Wired Equivalent Privacy قدیمی ترین پروتکل رمزنگاری **Wifi** است. [ایجاد شده در 1997]
- **ضعیف ترین سطح امنیت را دارد، چرا که رمزنگاری آن به سادگی قابل ردیابی و شکستن است.**
- **از الگوریتم RC4 جهت رمزنگاری data استفاده می کند.**
- **الگوریتم RC4، رمزنگاری را بر اساس رمزعبوری که برای کاربرها به عنوان SSID password تعریف می کنیم، انجام می دهد.**

نکته: SSID Password را با نام Authentication Key نیز می شناسیم.

- **پس به کلیدی که RC4 بر اساس Authentication Key، جهت رمزنگاری ایجاد و استفاده می کند، passphrase گفته می شود.**

نکته: شبکه ای که open authentication باشد، نمی تواند توسط WEP، رمزنگاری شود؛ چون passphrase وابسته به SSID Password است.

- **کلید passphrase، به حالت static یا ثابت باقی خواهد ماند، و همین static بودنِ passphrase، غیر ایمن است، چرا که اگر یک مهاجم به هرشکلی، این passphrase را شناسایی و پیدا کند، به سادگی قادر به دسترسی به تمامی ترافیک میان AP و Client خواهد شد.**
- **با توجه به اینکه به passphrase، همچنین** Pre-Shared Key **گفته می شود، این پروتکل را به شکل WEP-PSK نیز خطاب می کنند.**

پس از رفع مشکلات و باگ های موجود در WEP، در سال 2004**، پروتکل ترمیم یافته را** Wifi Protected Access (WPA) **نامیدند.**
این اولین نسخه ی WPA، همان WPA1 می باشد، که دارای دو نسخه ی Personal و Enterprise می باشد.

:WPA1 Personal

- **از الگوریتم RC4 جهت رمزنگاری data استفاده می کند.**
- **در این پروتکل، الگوریتم RC4، رمزنگاری را بر اساس یک کلید، به نام passphrase انجام می دهد که این کلید، static ، باقی نخواهد ماند.**
- **درحقیقت، passphrase اصلی، که در پایانه های ارتباط Wifi** (روی AP و روی Client) **تنظیم می کنیم، static خواهد ماند و آن را با عنوان Base Key خطاب می کنیم.**
- **اما از روی Base Key** (بر اساس Base Key)**، توسط یک پروتکل به نام TKIP** (Temporal Key Integrity Protocol)**، برای ارسال هر Packet در شبکه، یک passphrase خاص، تنظیم و به آن Packet اختصاص می یابد.** (Per-Packet Key System)

نکته: شبکه ای که open authentication باشد، نمی تواند توسط WPA1، رمزنگاری شود؛ چون passphrase وابسته به Base Key است.

- **پس Passphrase های ایجاد شده توسط TKIP، توسط RC4 رمزنگاری می شوند.**
- **پس مکانیزم رمزنگاری در WPA را با RC4-TKIP هم نشان می دهند.**
- **این پروتکل را با نام WPA-TKIP هم خطاب می کنند.**
- **این پروتکل را به شکل WPA-PSK نیز خطاب می کنند.**
- **خود پروتکل TKIP، عملیات** Message Integrity Check **را نیز انجام می دهد. یعنی صحت بسته ها را چک می کند.**
- **نقطه ضعف این روش این است که اگر یک مهاجم، به هرشکلی، Base Key** (یا همان SSID Password) **را پیدا کند، احتمال اینکه به روش های مختلف، passphrase های دیگر را که بر اساس آن هستند، شناسایی و پیدا کند نیز، بیشتر خواهد بود.**
- **گاهی با اینکه AP، قابلیت WPA را پشتیبانی می کند، اما از WEP استفاده می کنیم؛ به جهت عدم پشتیبانی برخی دستگاه ها از WPA!**

: WPA1 Enterprise

- **تحت این پروتکل، دستگاهی که سعی در ارتباط با AP دارد، باید پروتکل 802.1X را پشتیبانی کند، که می دانیم** Windows، MAC IOS و Linux **آنرا پشتیبانی می کنند.**
- **پس باید 802.1X را هم بر روی AP و هم بر روی End Device ، فعال کنیم.**
- **یک Radius Server در شبکه راه اندازی می کنیم.**
- **درحقیقت در این روش، جهت انجام رمزنگاری، نیاز به هیچ ارتباطی میان Client و AP نیست.**
- Client در اولین مرحله ی شروع ارتباط با AP، بطورخودکار به Radius Server وصل خواهد شد.
- **همه ی مراحل مدیریت encryption به عهده ی AAA Server** (Radius Server) **است، که با Client مکاتبه و هماهنگ می شود.**
- **استفاده از این پروتکل، ساختار پیچیده ای دارد، به همین جهت استفاده از آن در سازمان های بزرگ، منطقی تر است.**

نکته: شبکه ای که open authentication باشد، نمی تواند توسط WPA1، رمزنگاری شود؛ چون passphrase وابسته به Base Key است.

:WPA2

- سازمان Wi-Fi Alliance ، با تغییر پروتکل WPA به حالتی که بطورکامل با پروتکل 802.11i (که اتحادیه ی IEEE ایجاد کرده بود) مطابقت داشته باشد، پروتکل WPA2 را ایجاد و ثبت کرد. [ایجاد شده در 2007]
- علاوه بر اینکه امن تر از WPA1 است، یک سری قابلیت های جدید هم دارد.
- از الگوریتم AES (Advanced Encryption Standard) جهت رمزنگاری data استفاده می کند.
- بجای استفاده از TKIP، از پروتکل امن تری به نام CCMP استفاده می کند.
- این پروتکل را با نام WPA-CCMP هم خطاب می کنند.
- روش رمزنگاری در WPA2 را با AES-CCMP نشان می دهند.
- پروتکل WPA2 را به شکل WPA2-PSK نیز خطاب می کنند.
- قابلیت 802.1X را پشتیبانی می کند که تحت این قابلیت در WPA2، عملیات re-authentication سرعت بیشتری خواهد داشت.
- کاملن مشابه با WPA1، هم نسخه ی Personal دارد و هم نسخه ی Enterprise، که عملکرد هرکدام، مشابه آن در WPA1 است.

نکته: شبکه ای که open authentication باشد، نمی تواند توسط WPA2، رمزنگاری شود؛ چون passphrase وابسته به Base Key است.

:WPA3

- از الگوریتم AES جهت رمزنگاری data استفاده می کند.
- در این روش، Encryption هیچ ربطی به SSID password نخواهد داشت، چرا که در این روش، به ازای هر User، یک کلید رمزنگاری (Encryption Key) ایجاد و اختصاص داده می شود. (Per-User encryption)

نکته: وقتی شبکه را توسط WPA3 رمزنگاری کنیم، اگر بخواهیم می توانیم آن را در حالت Open Authentication نیز قرار دهیم و همچنان به شکل encrypted باقی بماند.

- حال که می توان شبکه را تحت این پروتکل، به شکل .Open Auth راه اندازی کرد، قابلیتی پدید می آید به نام Wi-Fi Easy Connect، که اتصال به شبکه را در زمینه ی IOT (اینترنت اشیا)، یا اتصال امنِ دستگاه های متفرقه به شبکه، بسیار آسان می کند.
- مزیت این روش این است که، اگر یک مهاجم، SSID Password را پیدا کند، همچنان قادر به دسترسی به ترافیک میان AP و Client ها نخواهد بود.
- فرض کنید، Client توسط یک encryption Key به AP متصل و یک Connection Session برقرار کرده است، سپس این ارتباط (Session) قطع و یا به پایان می رسد، و سپس از نو ارتباط را برقرار می کنند. پس در ارتباط دوباره، یک encryption Key جدید به این ارتباط اختصاص داده می شود. این encryption Key ها را Session Key هم می گویند، که متفاوت از یکدیگر خواهند بود.
- درحقیقت می دانیم که رمزنگاری که میان AP و Client انجام می شود، تنها بر روی سیگنال Data میان Client و AP انجام می گیرد، درحالی که سیگنالی که اطلاعات مدیریتی (management Frame) را میان AP و Client مبادله می کند، همچنان بطورجداگانه و بدون رمزنگاری باقی خواهد ماند، پس کافی ست که یک مهاجم بتواند به این کانال management نفوذ کند، به سادگی می تواند به شبکه رسوخ کند. اما یکی از ویژگی های پروتکل WPA3 این است که mangement Frame ها نیز رمزنگاری می شوند.
- می توان از این پروتکل، بدون 802.1X استفاده کرد و همچنان بالاترین سطح امنیت را حفظ کرد.
- پروتکلی که WPA3 جهت رمزنگاری استفاده می کند، SAE (Simultaneous Authentication of Equals) نام دارد.

: Wireless Issues

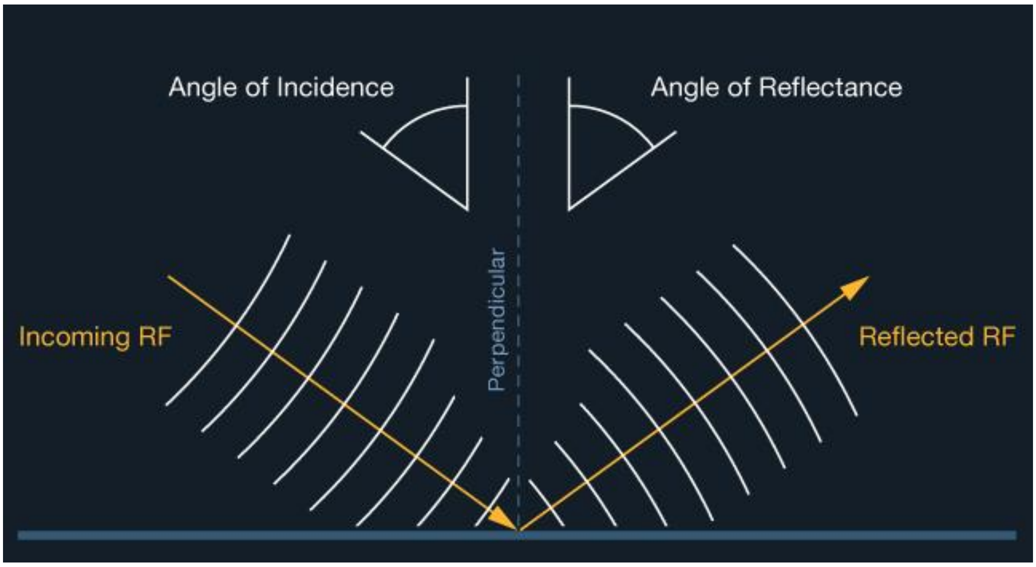
: Fading

وقتی امواج رادیویی با موانع فیزیکی برخورد می کنند، دچار fading می شود که شامل سه حالت است:

- **Reflection : بازتاب معکوس به سمت گیرنده است که به آن reflected گفته می شود.**

در شکل زیر، یک موج رادیویی فرود آمده را همراه با انعکاس آن پس از برخورد با یک جسم مسطح را می بینیم.

نکته: در این وضعیت، معمولاً زاویه ی فرود موج، و زاویه ی انعکاس آن، برابر هستند.

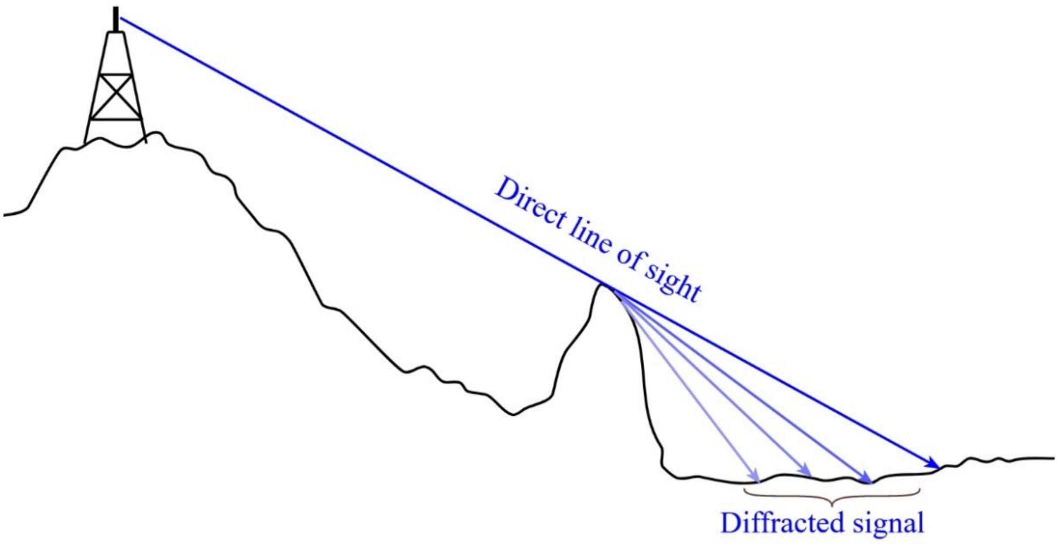


از اجسامی که امواج را به سادگی منعکس می کنند، آب (مثل روزهای بارانی) **و اجسام فلزی** (مثل کمدهای اداری) **هستند.**

- **Diffraction : به تجزیه ی یک جبهه از امواج، به امواج ثانویه ی ناخواسته، پراش گفته می شود، و به آن امواج، diffracted waves گفته می شود.**

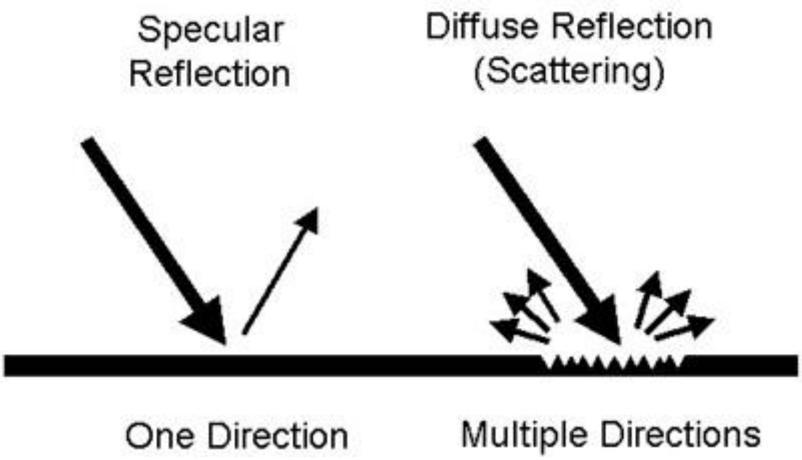
درحقیقت وقتی یک گیرنده در یک نقطه ی کور (Dead Zone) قرار بگیرد، به جای امواج اصلی و سالم، diffracted waves دریافت خواهد کرد.

مثلن در شکل زیر، می بینیم که موج ارسالی از دکل، پس از برخورد به صخره، دچار تضعیف شده است، به این دلیل که بخشی از آن، به جهت برخورد با صخره، خم شده و دچار تغییر مسیر می شود. به آن بخش از امواجی که دچار پراش شده اند، diffracted گفته می شود.



- **Scattering** : انتشار در جهات مختلف است که به آن **Scattered** گفته می شود.

حاصل این پدیده، شبیه به ترکیبی از **Diffraction** و **Reflection** می باشد. به این شکل که، امواج پس از برخورد با یک مانع، منعکس می شوند، اما در جهت های کاملاً مختلف و ناخواسته!



درحقیقت موج اصلی، پس از برخورد با مانع، به امواجی در چندین جهت متفاوت متلاشی می شود، که به سادگی سیگنال را تا حد از بین بردن، ضعیف می کند.

از موانعی که باعث **Scattering** می شود، می توان آب را نام برد.
حتی قطرات آب و رطوبت و یا حرارت زیاد موجود در هوا نیز، تا حدی باعث رخ دادن این پدیده بر روی امواج می شوند.

: Attenuation

درحقیقت، تضعیف، باعث **Signal loss** یا اتلاف سیگنال می شود.

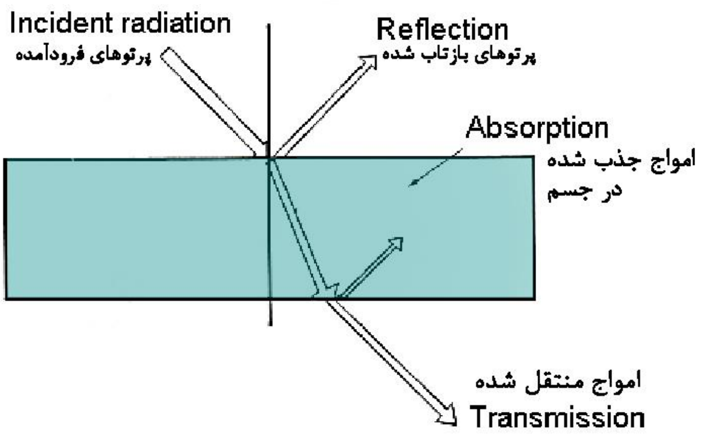
وقتی فاصله ی گیرنده و فرستنده زیاد باشد، تضعیف یا **Attenuation** رخ می دهد که برای پیشگیری از آن از یک تقویت کننده استفاده می شود:

- در شبکه های **digital** به آن **Repeater** گفته می شود.
- در شبکه های **Analog** به آن **Amplifier** گفته می شود.

Absorption (جذب): بخش زیادی از تضعیف، بر اثر برخورد با اجسام است، که بخش زیادی از انرژی موج، جذب اجسامی که بر سر راهش هستند، می شود.

- میزان جذب امواج در برخورد با اجسام مختلف را با واحد دسی بِل (**dB**) تعریف می کنیم.
- هریک **Decibel**، انرژی یک موج را به مقدار **20**٪ کاهش می کند.
- یعنی وقتی بگوییم مقدار جذب امواج در یک جسم، **5dB** است، یعنی احتمال این وجود دارد که پس از اینکه موج، با آن جسم برخورد کرد، بطورکامل از جذب شده و از دست برود.
- البته که هرقدر فرکانس یک موج بالاتر باشد، میزان جذب شدن آن در اجسام نیز بیشتر خواهد بود.

Building Material	2.4 GHz Attenuation	5 GHz Attenuation
Solid Wood Door 1.75"	6 dB	10 dB
Hollow Wood Door 1.75"	4 dB	7 dB
Interior Office Door w/Window 1.75"/0.5"	4 dB	6 dB
Steel Fire/Exit Door 1.75"	13 dB	25 dB
Steel Fire/Exit Door 2.5"	19 dB	32 dB
Steel Rollup Door 1.5"	11 dB	19 dB
Brick 3.5"	6 dB	10 dB
Concrete Wall 18"	18 dB	30 dB
Cubical Wall (Fabric) 2.25"	18 dB	30 dB
Exterior Concrete Wall 27"	53 dB	45 dB
Glass Divider 0.5"	12 dB	8 dB
Interior Hollow Wall 4"	5 dB	3 dB
Interior Hollow Wall 6"	9 dB	4 dB
Interior Solid Wall 5"	14 dB	16 dB
Marble 2"	6 dB	10 dB
Bullet-Proof Glass 1"	10 dB	20 dB
Exterior Double Pane Coated Glass 1"	13 dB	20 dB
Exterior Single Pane Window 0.5"	7 dB	6 dB
Interior Office Window 1"	3 dB	6 dB
Safety Glass-Wire 0.25"	3 dB	2 dB
Safety Glass-Wire 1.0"	13 dB	18 dB



Noise :

تأثیر امواج و خطوط دستگاه های دیگر بر سیگنال بکارگرفته شده مان می باشد.

- **هر گونه ارتباط رادیویی که در محدوده ی ISM باشد، می تواند مورد تداخل با باند های مجاورش قرار گیرد. یعنی در صورتی که ما از محدوده ی فرکانسی ISM استفاده کنیم و در مجاورت نیز، از این محدوده ی فرکانسی استفاده می شود، احتمال بالای بروز اختلال خواهد بود.**

چند عامل که سرعت WiFi را پایین می آورند:

- لامپ‌ها (چون نور هم مثل امواج رادیویی، در طیف امواج الکترومغناطیسی قرار دارد.) و یخچال‌ها
- WiFi دستگاه های دیگر یا مودم های دیگران
- حضور افراد در محیط و پیرامون مودم
- و به طور کل هر شئ فیزیکی، تا حدی باعث تضعیف سیگنال ها می شود.

- **قرار دادن یک Access Point در نزدیکی یک دستگاه اجاق ماکروویو، کاملاً کار اشتباهی خواهد بود.**
- **قرار دادن Router Access Point در گوشه های ساختمان نیز، برد سیگنال‌ها را کاهش می دهد.**

نکته: بهترین عملکرد سیگنال‌های Wireless در محیط‌های باز است، چون فراهم کردن محیط‌هایی تا این حد باز در محیط داخلی، غیرممکن است.

- **اگر آنتن قابل جداشدن باشد، می توان آن را با یک آنتن گیرنده ی قدرتمندتر تعویض کرد.**
- **Directional antenna یا آنتن جهت دار، سیگنال را فقط در یک جهت ارسال می کند و هر دستگاهی که بر سر راهش باشد، سیگنال را دریافت می کند.**

➢ Beamforming :

- به صورت کلی وقتی **Router**، سیگنال **Wi-Fi** را منتشر می‌کند، داده‌ها در تمام جهات پخش می‌شوند.
- قابلیت **Beamforming**، مکان **WiFi Client** را شناسایی کرده و سیگنال قوی‌تری را در آن جهت خاص ارسال می‌کند.
- **Router** های جدید امروزی با تکیه بر فناوری**Beamforming** ، بهبود کیفیت **Wi-Fi** و کاهش تداخل امواج را تضمین می‌کنند.
- **Beamforming** درباره ی تمرکز امواج بی‌سیم در یک جهت خاص است.
- تنها در صورتی از تمام مزایای **Beamforming** بهره‌مند می‌شویم که دستگاه‌های ما از استاندارد **802.11ac** پشتیبانی کنند. هم **Router** و هم **Client** باید از فناوری **Beamforming** پشتیبانی کنند.

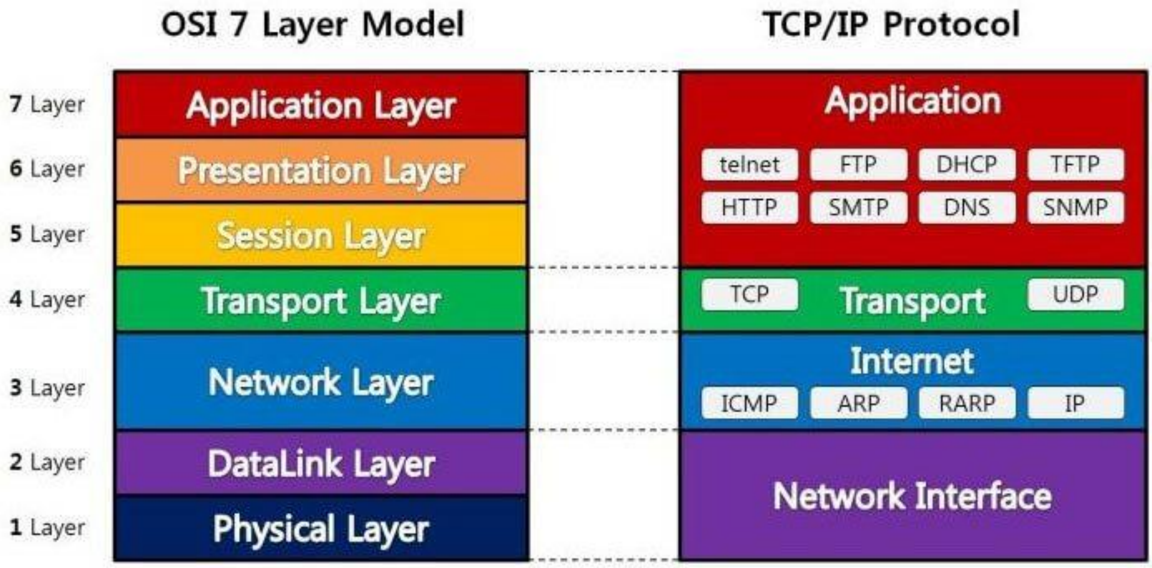


OSI (Open Systems Interconnection):

این مدل توسط سازمان ISO در سال 1984 به عنوان مدل مرجع شبکه، طراحی و ثبت شد.
توسط این مدل، انتقال داده ها از یک کامپیوتر به یک کامپیوتر دیگر، تشریح و تجزیه و تحلیل می شود.

در مدل Open System Interconnection یا همان OSI، پروتکلها در لایه های مختلف گروه بندی شده اند تا به سادگی بتوان کار هریک از آنها را شرح داد.

- مدل مرجع OSI دارای هفت لایه می باشد که پروتکل هایی که امور مشابه و خیلی مرتبط را انجام می دهند، در یک لایه ی یکسان قرار می گیرند.
- مدل OSI، فقط یک مدل تئوری می باشد، و به جز راحت نمودن توضیح کار پروتکلها، هیچ استفاده ی دیگری ندارد!



Physical : First Layer :

در این لایه که تنها تشکیل شده از سخت افزارهای لازم جهت انتقال اطلاعات می باشد، قراردادهای سخت افزاری اجرا می شوند.
وظیفه ی انتقال نهاییِ اطلاعات را دارد، به این صورت که ابتدا دادهها را به صفر و یک و سپس به سیگنال های الکتریکی تبدیل می‌کند.

- قالب بندی اطلاعات یا همان Encapsulation Unit در لایه ی فیزیکی، بر اساس Bit هاست.

: Secound Layer : Data Link

- آدرس IP قابل شناسایی نیست، بلکه با Mac Address کار می شود.
- درحقیقت لایه ی Data Link مسئولیت انتقال داده ها را در بستر فیزیکیِ شبکه بر عهده دارد.
- قالب بندی اطلاعات در لایه Data Link یا همان Encapsulation Unit در این لایه، بر اساس Frame است.
- سوئیچ های شبکه، در این لایه فعالیت می کنند.
- علاوه بر Switch ها، VLAN ها نیز در این لایه، کار می کنند.

Physical Addressing:

Physical Addressing با Network Addressing تفاوت دارد.
آدرس های شبکه ای که به Node های شبکه اختصاص داده می شوند و در شبکه می تواند مسیریابی شوند.
Network Addressing را با آدرس IP می شناسیم.
توسط Physical Addressing دستگاه ها را در همان رسانه ی فیزیکی (توسط MAC Address) از یکدیگر متمایز می کنیم.

Frame Sequencing:

Frame Sequencing این قابلیت را به Frame ها می دهد که اگر هنگام انتقال از ترتیب خارج شدند، در سمت گیرنده مجددا ترتیب گذاری شوند.

Flow Control:

مکانیزم Flow control یا کنترل جریان در لایه Data Link به دستگاه گیرنده این امکان را می دهد که Congestion در لینک را شناسایی کند و به دستگاه های Neighbor یا همسایه ی خودش این موضوع را اطلاع رسانی کند. دستگاه های Neighbor، اطلاعات Congestion را به پروتکل های لایه ی بالاتر بازبخش می کنند؛ از همین رو جریانی از ترافیک شبکه می تواند تغییر داده شود و یا Reroute شود.
کاربرد و کارکرد دیگر ویژگی Flow Control این است که گاهی سرعت فرستنده و گیرنده، تفاوت زیادی دارند، پس احتمال از دست رفتن داده های دریافتی زیادی وجود خواهد داشت، که در اینجا Flow Control به کمک آمده و سعی در حفظ روال موفق ارسال و دریافت می شود.

برخی پروتکل هایی که در لایه ی Data Link کار می کنند:

- ATM یا Asynchronous Transfer Mode
- PAgPیا Cisco Systems proprietary link aggregation Protocol
- PPP یا Point-to-Point Protocol
- CHAPیا Challenge Handshake Authentication Protocol
- CDPیا Cisco Discovery Protocol
- ARP یا Address Resolution Protocol
- LLDP یا Link Layer Discovery Protocol
- L2TP یا Layer 2 Tunneling Protocol
- و ...

: Third Layer : Network

بسیاری از تجهیزات و زیرساخت های شبکه مثل Router، و خیلی از پروتکل های زیرساختی شبکه، در این لایه کار می کنند.
تمرکز اصلی متخصصان زیرساخت شبکه نیز، روی لایه ی Network و پروتکل های آن است.

- در این لایه، بر روی Segment ها یا Datagram های دریافتی از لایه ی Transport، یک IP Address اضافه می کند.
- مهمترین وظیفه ی این لایه، مسیریابی Packet هاست. یعنی بهترین مسیر برای ارسال یک Packet تعیین می شود.
- از وظایف دیگر این لایه، آدرس دهی یا Addressing می باشد.
- مهم ترین دستگاهی که در این لایه کار می کند Router است.

پروتکل هایی که در لایه ی Network کار می کنند:
OSPF ، ICMP، IGMP، IPSec، ARP، EIGRP، RIP، IP و ... .
در آخر به این نکته اشاره کنیم که قالب بندی اطلاعات در لایه Network یا بعبارتی Encapsulation Unit این لایه بر اساس Packet است.
Router ها و همچنین سوئیچ های لایه سه، در این لایه کار می کنند.

: Fourth Layer : Transport

بطورخلاصه، عملکرد کلی لایه ی Transport، دریافت داده ها از لایه ی بالایی یعنی Session و شکستن آنها به قسمت های کوچکتر و تحویل آنها به لایه ی بعدی یعنی Network Layer می باشد.

پروتکل استفاده شده در این لایه، نوع Connection را مشخص می کند. TCP و یا UDP .

لایه ی Transport هشت وظیفه را بر عهده دارد :

1. Service Point Addressing:

Header لایه ی Transport شامل Service Point Address است که همان شماره ی Port سرویس مربوطه می باشد.

- لایه ی Transport با Service های شبکه، سر و کار دارد.

2. Segmentation و Reassembling:

وقتی لایه ی Transport یک بسته را از لایه ی Session دریافت کرد، آن را به قسمت های کوچک تری می شکنند.

اگر از پروتکل UDP استفاده کنیم، به این قسمت های کوچکتر، Datagram می گویند.

اگر از پروتکل TCP استفاده کنیم، به این قسمت های کوچکتر، Segment می گویند.

- هر Segment شامل یک شماره ی 32 بیتی به نام Sequence number است.

Sequence number به لایه ی Transport کمک می کند تا بتواند Reassembling بسته را انجام دهد.

Sequencing (شماره گذاری بسته ها) همچنین کمک می کند تا اگر یک بسته گم شد، بتوان آن را شناسایی و جایگزین کرد.

3. Connection Control:

شامل یکی از دو حالت زیر است:

- Connectionless: در صورت استفاده از پروتکل UDP.

هر Segment به عنوان یک Packet مستقل در نظر گرفته شده و به همان شکل در ماشین مقصد، به لایه ی Transport تحویل داده می شود.

- پروتکل UDP یا User Datagram Protocol در این لایه کار می کند.
- از این پروتکل برای انتقال بسته های اطلاعاتی صوتی و تصویری (در زمینه ی Media Streaming) که bandwidth و زمان و سرعت، اهمیت بالایی دارند، بسیار استفاده می شود.
- برای ارتباطات یکسو یا Broadcast بکار می رود.
- در صورت استفاده از TCP، هر ارسال و دریافتِ پیام Ack، خود باعث اشغال پهنای باند خواهد شد!
- پس در این روش، فقط به ازای هر Session ای که برقرار می شود (و نه به ازای هر Packet)، یک پیام تأییدیه ی ack از سمت مقصد به مبداء ارسال می شود.
- برقرار شدن یک Session، زمانی ست که همه ی Packet ها ارسال شدند.
- دقت و اطمینان بالایی از رسیدن و دریافت شدن Packet ها ندارد.

- Connection Oriented: در صورت استفاده از پروتکل TCP.

- قبل از تحویل دادن Packet ها از لایه ی Session به Transfort، یک Connection با لایه ی Transport ماشین مقصد برقرار می شود.
- پروتکل TCP یا Transmission Control Protocol در این لایه کار می کند.
- به ازای هر Packet که ارسال و در مقصد دریافت می شود، یک Confirmation یا Acknowledge به شکل یک Packet به نام Ack بر می گردد.
- اگر طی زمان مشخصی، پیام ack توسط مبدا دریافت نگردد، فرآیند ارسال Packet مجددا تکرار خواهد شد.
- TCP دقت بالایی دارد و reliable است.

- نسبت به UDP، سرعت انتقال اطلاعات بسیار پایین تر است.
- سرویس ها و پروتکل هایی که تحت TCP کار می کنند : FTP ، Telnet ، http ، SMTP ، POP3 و ... .
- ارتباط سه مرحله ای TCP، که اصطلاحاً TCP Handshake یا 3way Handshake هم گفته می شود:
  - Client درخواست هماهنگی را توسط یک Packet به نام Syn به مقصد ارسال می کند.
  - مقصد برای تأیید این درخواست، یک Packet به نام Syn/Ack را به Client پس می فرستد.
  - Client یک Packet به نام Ack را برای آغاز ارتباط به مقصد ارسال می کند.

  این ارتباط را بصورت Syn-Syn/Ack-Ack هم نشان می دهند.

- برخی سرویس ها می توانند بسته به نوع استفاده، هم تحت UDP و هم تحت TCP کار کنند. مثل: DNS

4. Flow Control:

عملیات Flow Control اطلاعات، بصورت End-to-End انجام می شود.

Flow control داده های ارسالی را بطورکامل کنترل و مدیریت می کند تا اگر حجم داده ها زیاد باشد Overflow رخ ندهد.

اگر داده ای در جریان ارسال، با خطا مواجه شد و یا ناقص ارسال شد، آن را اطلاع می دهد.

5. Error Control:

عملیات کنترل خطا یا Error Control نیز بصورت End-to-End انجام می شود و به شما این اطمینان را می دهد که اطلاعات دریافت شده بدون هیچ خطایی به مقصد رسیده اند.

6. Data Integrity:

یکپارچگی داده ها در دنیای امنیت اطلاعات، بسیار مهم است.

Data Integrity یعنی اینکه داده ها همانطوری که فرستاده شده اند، همانگونه هم توسط گیرنده دریافت شوند.

Data Integrity بوسیله ی Checksum انجام می شود.

7. Multiplexing:

مالتی پلکسینگ این امکان را فراهم می کند که در کامپیوتر بتوانیم بصورت همزمان از چند Service یا Application تحت شبکه استفاده کنیم.

مثلاً همزمان توسط پروتکل های http و ftp و smtp در حال تبادل اطلاعات هستیم، که این به جهت وجود Port هاست.

8. Byte orientation:

برخی از پروتکل ها، Byte stream ها را به جای Packet ها دریافت می کنند.

مثلاً پروتکل UDP این مزیت را دارد که بتوان Voice را در بستر پروتکل IP انتقال داد.

: Fifth Layer : Session

زمانیکه دو کامپیوتر بخواهند با همدیگر به برقراری ارتباط بپردازند، ابتدا باید یک Session بین آنها ایجاد شود تا بتوانند منابع خود را به اشتراک بگذارند.

هدف و وظیفه ی اصلی لایه ی Session :

- ایجاد و برقراری (establishment) و
- مدیریت (maintaining and management) و
- هماهنگ سازی (Synchronization) و
- پایان دادن (ending a Session)

ارتباط میان دو Application یا Service است که می خواهند با یکدیگر تبادل اطلاعات داشته باشند.

عملکرد لایه ی Session در سه فاز یا عملیات به انجام می رسد:

- **Dialog Control** : این لایه تعیین می کند که ارتباط بصورت **Half-Duplex** باشد یا **Full-Duplex**.
- **Token Management** : این لایه باعث می شود که دو سیستم بصورت همزمان اقدام به انجام عملیات حساس نکنند تا تداخل کاری بین دو سیستم بوجود نیاید.
- **Synchronization** : این امکان را می دهد که یک **Checkpoint** از وضعیت فعلی فرآیند درون **Data Stream** تحت **Session** ایجاد شود. مثلاً اگر سیستم در حال ارسال یک فایل **800** صفحه ای باشد، پیشنهاد می شود که به ازای هر **50** صفحه، یک **Checkpoint** ایجاد شود. حال اگر بعد از ارسال **110** صفحه، سیستم **Crash** کرد، دیگر نیاز نیست که از صفحه ی یک، دوباره اقدام به ارسال صفحات کند.

این سه فاز، از وظایف پروتکل **X.225** می باشند.

لایه ی **Session** در استفاده از **Web Conferencing** و **Live TV** و بطور کلی **Media Streaming** بسیار نقش مهمی دارد.

از دیگر پروتکل هایی که در این لایه فعالیت می کنند:

- **Apple Talk**
- **Zone Information Protocol**
- **L2TP**
- **RPC**
- **PPTP**
- **PAP**
- **iSNS**
- **NetBIOS**

قالب بندی اطلاعات در این لایه (**Encapsulation Unit**) بر اساس **Data** است.

:Sixth Layer : Presentation

نام دیگر این لایه، Translation می باشد.
لایه Presentation مسئول Formatting (قالب بندی) و ارائه ی اطلاعات برای لایه ی Application می باشد.
مثلاً فرمت نمایش فایل های عکس مثل PNG ، JPG و ... در این لایه تعریف می شوند.
و این فرمت بندی در لایه ی Presentation برای نوع داده های دیگر مثل متنی و صوتی و ... نیز صدق می کند.
رمزنگاری داده ها (Data Encryption) نیز در این لایه انجام می شود.
همچنین فشرده سازی داده ها (Data Compression) نیز در این لایه انجام می شود که تا حدودی در پهنای باند شبکه صرفه جویی شده و سرعت انتقال اطلاعات نیز تا حدی بالا می رود.

داده ها در این لایه، بصورت Data ارسال و دریافت می شوند.

:Seventh Layer : Application

99 درصد پروتکل ها در این لایه کار می کنند.

مثلاً می خواهیم:

- **در شبکه Email بفرستیم؛**
- **بین Client ها، فایلی را به اشتراک بگذاریم؛**
- **از یک Website بازدید کنیم؛**

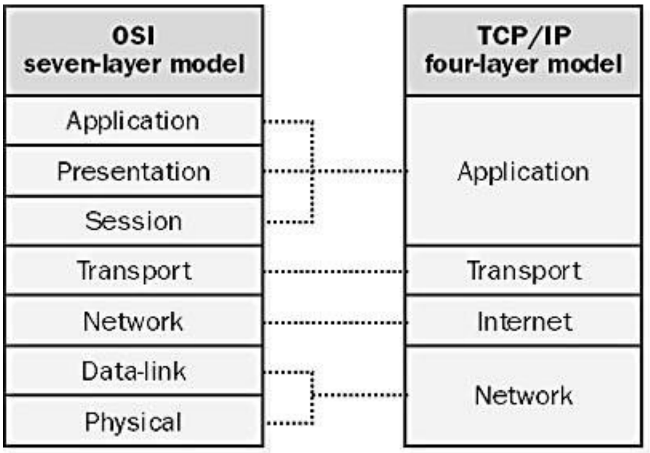
همه ی این امور در لایه ی Application انجام می شوند.
در حقیقت، تمامی اموری که در این لایه انجام می شوند، نیازمند محیط سیستم عامل هستند، یعنی این لایه، تحت محیط OS کار می کند.

برخی پروتکل های این لایه، عبارتند از:
Web Service، DNS، DHCP، Mail، FTP، HTTP، SMTP، SNMP، POP3 و ... .

داده ها در این لایه نیز، بصورت Data ارسال و دریافت می شوند.

:(Transmission Control Protocol) TCP/IP

درحقیقت مدل OSI یک مدل تئوری است جهت درک جزئی تر از ارتباطات شبکه ای.
در دنیای واقعی، مدل مورد استفاده برای مخابره ی اطلاعات، مدل چهار لایه ای TCP/IP است.



مدل TCP/IP :

- Open nature است، یعنی رایگان.
- Flexible است، یعنی بر روی هرگونه سیستم عاملی و هرگونه سخت افزار شبکه از هرنوع مدلی، قابل راه اندازی و استفاده است.
- به سادگی با انواع شبکه های کوچک و بزرگ، قابل هماهنگی و پیاده سازی است.

تقریباً تمامی ویژگی ها و عملیات در لایه ی انتقال TCP/IP مشابه با لایه ی انتقال OSI می باشد.

: fourth Layer : Application

- Encapsulation Unit در این لایه، Message نامیده می شود.
- پروتکل های مهمی مثل DNS و DHCP در این لایه کار می کنند:

➢ HTTP , HTTPS :

- HTTP جهت انتقال انواع مختلف داده، تحت صفحات وب، بکار می رود.
- اینکه داده های منتقل شده، از محیط اینترنت باشند یا نباشند، مهم نیست، هر تبادل داده ای که توسط مرورگرهای Web انجام شود، توسط این پروتکل خواهد بود.
- HTTPS همان HTTP است که S، مخفف Secure است! به این معنی که پروتکل HTTP ای که توسط SSL، امن شده است.
- پروتکل SSL از Certificate ها جهت تضمین امنیت استفاده می کند.
- نمی توان جهت انتقال فایل های بسیار بزرگ، از آن استفاده کرد.
- جهت ارسال و دریافت ایمیل توسط Web mail ها نیز کارآیی دارد.
- http از پورت 80 استفاده می کند.
- https از پورت 443 استفاده می کند.

➢ FTP (File Transfer Protocol):

- FTP جهت انتقال فایل میان انواع ماشین ها (کامپیوترها) بکار می رود.
- سرعت بالاتر و پیچیدگی کمتری نسبت به HTTP دارد.
- می توان جهت انتقال فایل های بسیار بزرگ، از آن استفاده کرد.
- از پورت های 20 و 21 استفاده می کند.

➢ IMAP, POP, POP3:

- جهت دریافت ایمیل استفاده می شوند.
- POP3 از پورت 110 استفاده می کند.
- IMAP از پورت 143 بصورت unencrypted و پورت 993 بصورت encrypted استفاده می کند.

➢ SMTP:

- جهت ارسال ایمیل استفاده می شود.
- از پورت 25 استفاده می کند.

➢ Telnet:

- جهت برقراری یک ارتباط command line ای با یک کامپیوتر عضو شبکه، از راه دور بکار می رود.
- امنیت خیلی زیادی ندارد.
- برخی نرم افزارهایی که تحت Telnet کار می کنند: PuttY و SecureCRT
- از پورت 23 استفاده می کند.
- برای آغاز یک ارتباط Telnet تحت ویندوز، در cmd دستور telnet را وارد می کنیم.

➢ SSH (Secure Shell):

- فرض کنید بخواهیم از راه دور، به تنظیمات یک Router یا managed Switch و یا یک Access Point، متصل شده و آنها را اصلاح کنیم، پس از پروتکل SSH استفاده می کنیم.
- کاملاً مشابه با Telnet عمل می کند، با این تفاوت که رمزنگاری شده است (**encrypted**)
- از پورت 22 استفاده می کند.

Third Layer : Network (Link Layer):

- Encapsulation Unit در این لایه، Frame نامیده می شود.
- برخی پروتکل های مهم این لایه:
  - PPP (Point to Point Protocol):
    - جهت کدگذاری داده های خطوط Serial استفاده می شود.
    - سرعت را تنظیم می کند.
    - نوع رمزنگاری و احراز هویت را تنظیم می کند.
  - SLIP (Serial Line Internet Protocol):
    - جهت کدگذاری داده های خطوط Serial استفاده می شود.
    - برخی ویژگی های PPP را ندارد، مثل Error correction و ... .
  - Ethernet:
    - بطورساده، Ethernet یک خط اشتراکی است که توسط آن، چند سیستم با یکدیگر مرتبط بوده و تبادل داده می کنند.
    - شبکه های LAN یک Ethernet هستند.
    - از طرف IEEE استاندارد 802.3 برای ایجاد و اختصاص داده شده است.

Port mirroring :

گاهی که در شبکه، یک سیستم کنترل امنیت (مثل IDS یا IPS) را توسط switch یا Router به شبکه متصل می کنیم، نیاز است که این سیستم امنیتی، قادر به دریافت اطلاعات و مشاهده ی همه ی ترفیک های ورودی و خروجی همه ی پورت های آن Switch یا Router باشد.

پس از port mirroring استفاده می کنیم که به این شکل عمل می کند که از همه ی تبادلات داده ی همه ی Port ها، یک کپی به پورتی که سیستم امنیتی به آن متصل است، ارسال می شود.

نکته: قابلیت Port Mirroring تنها در Switch های managed قابل راه اندازی است.

به قابلیت Port Mirroring:

- در Switch های Cisco گفته می شود: SPAN (Switched Port Analyser)
- در Switch های 3COM گفته می شود: RAP (Roving Analysis Port)

اگر Port Mirroring فقط مربوط به local Switch باشد، به این قابلیت Local Mirror گفته می شود.

اگر Port Mirroring علاوه بر local Switch، ترافیک های پورت های Switch های دیگری را نیز دریافت کند، به آن Remote Mirror گفته می شود.

در حالت Remote Mirror در سوییچ های Cisco، به آن RSPAN گفته می شود.

درحقیقت، توسط Port Mirroring، همه ی Packet های پورتهای دیگر به همراه محتویات آنها، بطورکامل، به سوی mirrored Port ارسال می شوند؛ که در این صورت، حجم ترافیکی که به سوی این Port ارسال می شود، خیلی بالا خواهد بود و سیستم متصل شده به mirrored Port نیز باید دارای فضای ذخیره سازی کافی نیز باشد.

اما توسط قابلیتی به نام NetFlow می توان تعیین کرد که محتوای این Packet ها کسر شده و تنها Meta data مربوط به Packet ها به سوی mirrored Port ارسال شود.

:Remote desktop

- هر کامپیوتر یک IP دارد.
- در هر کامپیوتر، یک یا چند **Account** (**username** و **password**) می توانند جهت ورود به آن، موجود باشند.
- **Account** ها در گروه بندی های مختلفی قرار می گیرند. مثلاً **Administrator** ها و یا **User** های معمولی و ... .

ساده ترین و دم دست ترین ابزار جهت متصل شدن به یک کامپیوتر ویندوزیِ عضو شبکه، بدون اینکه پشت آن کامپیوتر نشسته باشیم، **Remote desktop** می باشد.

ابتدا باید مشخصات یک **Account** که در **Windows** آن سیستم وجود دارد را داشته باشیم (username و password):

- آن **Account** باید حتماً عضو یکی از گروه های **Remote Desktop Users** یا **Administrators** باشد.
- **Account** ای که فقط عضو گروه **Users** باشد، از این قابلیت محروم است.

پس باید وقتی با آن **Account** وارد سیستم شدیم، در **Control Panel** >**System** >**Remote Control** ، تیک این قابلیت (Allow Remote Connections to this Computer) برای آن فعال شده باشد.

- پورت **Remote Desktop** برابر است با: **3389** .
- **Remote Desktop** با پروتکل **RDP** کار می کند. (**Remote Desktop Protocol**)
- برای باز کردن سریع برنامه ی **Remote Desktop** ، در **Run** تایپ می کنیم: **mstsc**
- در **Windows** می توان به طور همزمان با چند **PC** ارتباط **Remote Desktop** برقرار کرد.
- نرم افزارهایی هستند که به شکل راحت تر و با امکانات بیشتری، امکان **Remote Connection** را فراهم می کنند، مثل **VNC** که باید در سیستم مقصد، از قبل نسخه ی **VNC Server** نصب و فعال بوده باشد؛ تا بتوان به راحتی و با وارد کردن فقط **IP** آن و پسوردی که در نرم افزار **VNC** آن تنظیم شده است، به آن متصل شد.

نرم افزارهای قدرتمند **Remote Connection** دیگر:

- Team Viewer
- Any Desk

تصور کنید در خانه یا اداره که همه ی دستگاه های موجود، به یک **Modem Router** متصل شده اند، قصد داشته باشیم، دو کامپیوتر را از طریق **remote** به یکدیگر متصل کنیم.

به راحتی از طریق **Remote Desktop Connection** و یا برنامه هایی مثل **VNC** یا **AnyDesk** می توان این ارتباط را برقرار کرد.

محدودیت ها:

- نیاز است که در هر سیستم، برنامه ی **VNC** یا **AnyDesk** نصب باشد.
- در مورد برنامه ی **VNC** نیاز است که پسورد **VNC** ای که در برنامه ی مقصد ثبت شده است را داشته باشیم.
- در مورد برنامه ی **AnyDesk** نیاز است که هنگام درخواست اتصال، درخواست ارتباط را در مقصد، تایید کنیم.
- در مورد برنامه ی **Remote Desktop** نیاز است که در اولین ارتباط از راه دور، **username** و **password** یکی از حساب های کاربری در مقصد را داشته باشیم.
- در مورد برنامه ی **Remote Desktop**، پس از برقراری ارتباط با سیستم مقصد، کنترل از دست خود کاربری که در مقصد پشت سیستم نشسته است خارج شده و او فقط صفحه ی **logout** شده ی ویندوز را می بیند!

اما تصور کنید که بخواهیم ارتباط Remote را، از دو شبکه ی متفاوت، انجام دهیم.
مثلاً ارتباط میان موبایلی که از اینترنت سیم کارتش استفاده می کند، با یک کامپیوتر که از اینترنت مودم خانه استفاده می کند؛ و یا ارتباط میان لب تاپی که در خانه است و کامپیوتری که در اداره است.
در این حالت، چون دو طرف، در دو شبکه ی متفاوت و با IP های متفاوت هستند، ابتدا نیازمند این هستیم که هر دو طرف مبدا و مقصد را وارد یک شبکه کنیم. (به هردو طرف، آدرس IP هایی که در یک شبکه هستند، اختصاص بدهیم.)
که این یکسان سازیِ آدرس هردو طرف، توسط یک کانال امن انجام می شود، که همان VPN است.
سپس می توان به شکل معمول، از طریق یکی از برنامه هایی که در بالا گفته شد، Remote Connection را برقرار کرد.

Windows :

- ✓ یک سیستم عامل 32 بیتی (86x)، حداکثر Ram تا میزان 4GB را پشتیبانی می کند.
- ✓ یک سیستم عامل 64 بیتی (64x)، حداکثر Ram تا میزان 16EB را پشتیبانی می کند.
- ✓ حداقل میزان Storage موردنیاز برای نصب windows، برای 32bit برابر است با 16GB و برای 64bit برابر است با 20GB .
- ✓ منظور از patch the OS، انجام به روز رسانی های سیستم عامل است.
- ✓ منظور از dispatch a technician، اعزام یک فنی کار است.

- **برخی دکمه های میانبر ویندوز:**

ورود به Task manager	Ctrl+Shift+Esc
ورود به پنجره ی System	This PC را انتخاب کرده و Alt+Enter
ایجاد Desktop جدید	Ctrl+WIN+D
حرکت میان Desktop ها	Ctrl+WIN+Left/Right
بستن یک Desktop	Ctrl+WIN+F4
Minimize کردن همه ی پنجره های باز	WIN+D
کوچک و بزرگ کردن اندازه ی آیکون های desktop	Alt+Ctrl+(+/-)
باز کردن یک Windows Explorer	WIN+E
تنظیم نوع نمایش تصویر در زمان اتصال بیش از یک مانیتور	WIN+P
ورود به Windows Settings	WIN+I
ورود به کنسول جستجوی RUN	WIN+R
شروع ضبط/قطع ضبط ویدیو از محیط ویندوز	WIN+Alt+R
مشاهده ی ویدیوهای ضبط شده	WIN+G

- جهت ورود به یک **local account** روی یک کامپیوتری که عضو **domain** است، **username** را به یکی از دو شکل زیر پُر می کنیم:
  - HOSTNAME****LocalAccountName
  - .****LocalAccountName
- وقتی به آدرس ٪systemroot٪ اشاره می کنیم، درحقیقت منظور همان **C:\\Windows** می باشد، و یا اگر ویندوز در درایو **D** نصب باشد، به معنی **D:\\Windows** خواهد بود.
- اگر در تنظیمات **Windows Defender** ، محافظت بصورت **real Time** را غیرفعال کنید، دوباره به صورت خودکار فعال می شود تا از امنیت سیستم مطمئن باشد.
- جهت به روزرسانی **Driver** مربوط به کارت گرافیک، بهترین کار این است که جدیدترین نسخه را از سایت خود سازنده ی آن کارت گرافیک دریافت و نصب کنیم؛ اما نیاز به دانستن دقیق نسخه و مدل کارت گرافیک است، پس در **Run** درج می کنیم: dxdiag و در تب **Display** مدل دقیق آن را پیدا می کنیم.
- اگر بخواهیم روی یک سیستم که به عنوان یک **Kiosk PC**، تنها جهت کار با یک نرم افزار و یا فقط جهت تعامل با مشتری تنظیم شده باشد، و در صورت خاموش-روشن شدن، بطورخودکار و بدون **Password** دوباره وارد شود، از **Guest User** استفاده می کنیم.
- بطورمعمول فایل های **dll.** که فایل های سیستمی **Windows** هستند، توسط خود ویندوز، بطور پیشفرض مخفی می شوند، و برای ظاهر شدن آنها، باید به **Folder options** رفت.
- فرض کنید فایلی را از یک **NTFS Partition** به یک **NTFS Partition** دیگر منتقل کنیم. **Permission** های روی این فایل به این صورت خواهند شد که هم **Permission** های قبل را حفظ کرده و هم **Permission** های درایو جدید را دریافت می کند.
- وقتی یک نرم افزار یا یک فایل اجرایی، با ویندوز ورژن جدید، سازگار نبوده و اجرا نمی شود یا با اشکال اجرا می شود، می توان آن را به صورت **run in a compatibility mode** اجرا کرد.
- ابزار **Performance monitor** یک ابزار کاملاً ساده جهت، پیگیری و چک کردن وضعیت کارکرد یا میزان بکارگیری بخش های مختلف سیستم مثل **CPU** ، کارت گرافیک، **Ram** (Memory)، **Storage** (Physical Disk)، **NIC** (Network Adapter) و ... است.
- جهت دریافت **Hostname** یک سیستم و بررسی اینکه مجازی یا فیزیکی است، وارد **PowerShell** شده و:

```
Get-wmiobject -computer LocalHost win32_computersystem
```

: (cmd) Command Prompt

برای ورود به این کنسول، کافی ست در کنسول جستجوی RUN وارد کنیم: cmd

- **برای باز کردن پنجره ی cmd در حالت Boot سیستم:**
  - سی دی ویندوز را وارد می کنیم و به صفحه ی نصب ویندوز می رویم.
  - دکمه های ترکیبی shift + F10 را می فشاریم.

- **برای مشاهده ی همه ی دستورات موجود در cmd از دستور help کمک می گیریم.**
  - اگر بعد از دستور help نام یک دستور دیگر را بنویسیم، تمام اطلاعات مربوط به دستور دوم را نمایش می دهد؛
  - درج دستور /? بعد از دستور موردنظر، کاملاً کار دستور help را انجام می دهد.

نام درایو:	تغییر مسیر cursor به درایو دیگر
Cls	پاک کردن تمام محتویات موجود در صفحه
Color	تغییر رنگ متن در صفحه | بعد از آن باید یکی از شانزده ارقام هگزادسیمال را وارد کرد
Date	نمایش یا تغییر تاریخ
systeminfo	اطلاعات سیستم را نشان می دهد.
Wmic [اینتر] baseboard	برای پیدا کردن مدل و Serial Number و مشخصات دیگر Laptop
powercfg /batteryreport /output "d:\battery_report.html"	دریافت آمار و مشخصات باطری و برق Laptop
Tree	پوشه های موجود در آدرس پشت سرش یا آدرس مقابلش را به شکل درختی نشان می دهد
Type	محتویات فایل متنی که نامش یا آدرسش در مقابل می آید یا در پشتش قرار دارد را نشان می دهد
*.[پسوند]	برای فراخوانی و کار روی همه ی فایل ها با پسوندی خاص، آنها را به این شکل فراخوانی می کنیم.
dir *.pdf	جستجوی همه ی فایل های PDF در مسیری که Cursor قرار دارد.
dir /p *.pdf	جستجو و نمایش صفحه به صفحه ی همه ی فایل های PDF در مسیری که Cursor قرار دارد
dir /s *.pdf	جستجوی همه ی فایل های PDF در مسیری که Cursor قرار دارد و در تمام پوشه ها و زیرپوشه ها
start نام فایل.پسوند	فایل ها را اجرا می کند.
copy d:\آدرس فایل یا پوشه c:\آدرس فایل یا پوشه	Copy کردن یک فایل
move d:\آدرس فایل یا پوشه c:\آدرس فایل یا پوشه	Cut کردن یک فایل
Md [نام درایو]:\ [نام پوشه]\ [نام پوشه]	ایجاد پوشه های تودرتو
Mkdir [نام درایو]:\ [نام پوشه]\ [نام پوشه]	
Rd [نام درایو]:\ [نام پوشه]\ [نام پوشه]	حذف یک فایل یا پوشه
ren [نام فعلی پوشه یا فایل با پسوند] [نام جدید برای پوشه یا فایل با پسوند]	تغییرنام
fsutil file createnew i:\myfile.txt 2000000000	ایجاد یک فایل متنی با هر حجم دلخواه

- **برای تغییر مسیر Cursor در cmd به مثلاً آدرس یک فایل:**
  - ابتدا آدرس آن فایل را درAddress Bar کپی می کنیم. سپس در cmd وارد درایو فایل مورد نظر می شویم. مثلاً : G:

G:/>

  - سپس کافی ست کلمه ی CD را با یک فاصله درج کرده و با کلیک راست، آدرس فایل را paste کرده و وارد کنیم.

- **حذف یک برنامه توسط cmd :**
  - ابتدا cmd را با دسترسی مدیریتی باز کرده و دستور زیر را وارد می کنیم:

wmic

  - برای مشاهده ی نام کامل و صحیح نرم افزار موردنظر، دستور زیر را وارد می کنیم تا همه را لیست کند:

Product get name

  - حال برای حذف کردن برنامه ی موردنظر، از دستور زیر استفاده می کنیم:

Product where name=”XXXXX” call unistall

  - و در پایان حذف آن، باید خطی مشابه ”Method Execution Successful“ را در خروجی دریافت کنیم.

همانطور که در جدول بالا می بینیم، دستور کپی کردن، **Copy** است.
اما پس از آن یک ابزار قوی تر ابداع شد، به نام **xcopy** که طرز کار با آن مشابه با **copy** است، اما قدرت و سرعت و گزینه های بیشتری دارد.
و پس از **xcopy** ، یک ابزار قوی تر با سرعت و قدرت و گزینه های بیشتری ابداع شد به نام **robocopy**.

یک کپی ساده: توسط دستور زیر، همه ی محتویات پوشه ی **Folder1** درون پوشه ی **Folder2** کپی می شوند.(حتی محتویات **hidden** را)

robocopy D:\Folder1 E:\Folder2

نکته: اگر در آدرس مقصد، پوشه ی **Folder2** وجود نداشته باشد، آن را ایجاد خواهد کرد.

نکته: اگر برای آدرس مقصد، نام پوشه را درج نکنیم، همه ی محتویات پوشه ی **Folder1** را درون خود درایو **E** می ریزد!

نکته: همچنین جهت کپی شدن همه ی زیرپوشه های موجود در **Folder1**، می توان از پارامتر **/S** در پایان دستور استفاده کرد، که اگر بخواهیم همه ی **Subfolder** ها را کپی کند، حتی آنها که پوشه ی خالی هستند، از **/E** استفاده می کنیم.

نکته: اگر روی فایلها یا **Directory** ها مجوز (**Access Control List**) تنظیم باشد و حساب کاربری مان، توانایی دسترسی به فایلها را نداشته باشد، می توان از پارامتر **/B** استفاده کرد تا محتویات موردنظر با مجوز **SeBackupPrivilege** و **SeRestorePrivilege** خوانده و در مقصد نوشته شوند.

Timestamp:

همانطور که می دانیم وقتی وارد **Properties** یک فایل می شویم، در تب **General**، سه گزینه ی در مورد تاریخ وجود دارد:

- **Created**
- **Modified**
- **Accessed**

به این سه گزینه، **Timestamp** آن فایل گفته می شود.

- توسط دستور **robocopy** می توان نوعی **Backup** را تنظیم نمود، که در هربار **Backup**، تنها از فایل هایی که تغییر پیدا کرده اند، **Backup** ایجاد شود. (یا به قولی تنها آن فایل هایی، نسخه ی مبداشان تغییر کرده اند را، رونویسی (**overwrite**) کند و بقیه را بی تغییر رها کند.)

  که این کار توسط بررسی **Timestamp** های فایل ها انجام می شود، که جزیی از **option** های **robocopy** می باشد.
  و در علم **Backup** گیری، به این نوع، **Incremental Backup** گفته می شود.

- توسط دستور **robocopy** بطور پیشفرض از همه ی محتویاتی که بصورت **hidden** هستند نیز کپی گرفته می شود.
  یعنی توسط **robocopy**، یک کپی **100** درصدی خواهیم داشت.

:AppData folder

بطورمعمول، این یک پوشه مخفی است که می توان آن را توسط تنظیمات Folder options آشکار کرد.
برای هر User account در ویندوز، یک پوشه ی AppData (مخفف Application Data) **وجود دارد، به این شکل که در مسیر زیر قرار دارد:**
C:\Users\USERACCOUNT\AppData\
روش دسترسی سریع تر، درج عبارت %appdata% در Run یا نوار آدرس file explorer است که البته به مسیر زیر هدایت خواهد شد:
C:\Users\USERACCOUNT\AppData\Roaming
بطورکلی پوشه ی AppData شامل اطلاعات و تنظیمات مربوط به نرم افزارهاست.
مثلاً نرم افزار firefox، اطلاعات جستجو و Bookmark های کاربر را در پوشه ی Roaming ذخیره می کند. که می توان این اطلاعات را از کامپیوتر جاری به یک کامپیوتر دیگر منتقل کرد.

اگر نیاز داشته باشیم که از تنظیمات خاص یک نرم افزار محافظت کنیم، پس نیاز خواهد بود که از محتویات این پوشه نیز Backup تهیه کنیم؛ درغیر اینصورت، نیازی به تهیه ی Backup از این پوشه نیست.

نکته: برای افزایش سرعت یک سیستم local هم گاهی می توان تمام محتویات این پوشه را حذف کرد؛ که البته پس از آن، در مرورگرهای سیستم، از همه ی وبسایت هایی که در آنها login کرده بودیم، logout صورت خواهد گرفت.

Event Viewer :

در حقیقت بکارگیری Firewall ها و سیستم‌های تشخیص نفوذ، تنها به افزایش ضریب امنیت در خصوص حملات خارج از سازمان کمک می‌کنند و تنها راه برای شناسایی تهدیدات داخلیِ سازمان، نظارت یکپارچه بر گزارش های سیستم‌عامل می‌باشد.
درحقیقت این گزارش ها، دارای یک کد هستند، که به آن generic error code گفته می شود، و تنها جایی که می توان آنها را بررسی کرد، Event Viewer می باشد.

- گزارش ها یا همان Log ها حاویِ اطلاعات بسیار حساس و حیاتی از همه ی رویدادهای مربوط به برنامه‌های کاربردی (Application)، سرویس‌ها (Service) و سیستم عامل (OS) می‌باشند.
- اطلاعات ثبت شده در Log ها، به ما در شناسایی خطاها و تهدیدات امنیتی و عیب یابی آنها و البته آگاهی از تغییرات سیستم، کمک می کنند.
- Log ها با فرمت باینری در فایل‌هایی با پسوند Evt. ذخیره می‌گردند.

گزارش ها به طوراساسی، سه دسته هستند:

- **Information** : در یک مورد خاص، اطلاعاتی می دهد.
- **Warning** : در یک مورد خاص، احتمال وقوع خطایی را اطلاع می دهد.
- **Error** : خطایی که در یک موردخاص رخ داده است را گزارش می دهد. (همیشه خطرناک نیست!)

پس ابتدا در این کنسول، از سمت چپ، وارد **Windows Logs** می شویم.
بطورکل، در پوشه ی **Windows Logs**، و در همه ی پوشه های مشابه دیگر، **Log List** هایی وجود دارند، که گزارش های متفاوتی از **Log List** های دیگر را دریافت و نگهداری می کنند.

مهم ترین یا عمومی ترین **Log List** ها، در پوشه ی **Windows Logs** هستند.
Application Log : شامل گزارش هایی در مورد نحوه ی عملکرد نرم افزارها می‌باشد.
پس برنامه‌ها، خطاها یا اعلان های خود را در این لاگ ثبت می‌کنند.
Security Log :

- تلاش‌های موفق یا ناموفق ورود به سیستم (Authentication Logs)
  - جهت استفاده از قابلیت، ابتدا باید آنرا فعال کرده باشید، که در اینجا بتوان گزارش های آن را دید.
  - جهت فعال سازی آن، وارد **Group Policy** شده (در **Run** درج می کنیم: gpedit.msc) و به مسیر زیر می رویم:

Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy

  - در سمت راست روی گزینه ی Audit logon events دو بار کلیک می کنیم.
  - در صفحه ی باز شده، هر دو گزینه ی **Success** و **Failure** را فعال می کنیم.

بطورمعمول، ورودهای موفق با **Keyword** برابر با **Audit Success** و **Event ID** برابر با **4624**،
و ورودهای ناموفق با **Keyword** برابر با **Audit Failure** و **Event ID** برابر با **4625** ذخیره می شوند.
مثلاً در کادر پایین در تب **General**، به خوبی می توان برای **Failure Information** دلیل شکست در ورود را دید.
و یا در پایین کادر، می توان در مقابل **Logged** ، تاریخ و ساعت دقیق آن رخداد را مشاهده کرد.

- خروج از حالت **Sleep Mode** و ...
- تغییر تنظیمات **Policy** های سیستم،
- تغییر فایل‌های حساس.

این **Log** در سیستم های **Server**، دارای اطلاعات حساس و مهمی است، و نظارت یکپارچه و دائمی بر آن یکی از الزامات مدیران شبکه است.

System : شامل اطلاعات مربوط به سلامت سیستم می باشد؛

- مانند خطای روشن و خاموش شدن سیستم،
- ثبت ورود به **Sleep Mode**
- تغییر ساعت و تاریخ
- خطا یا اعلان **Update** مربوط به سخت افزارها
- **Start** و **Stop** شدن سرویس ها

Setup :

- شامل اطلاعاتی درباره ی نصب و به‌روزرسانی ویندوز است.
- هر رویدادی که به نصب یک بسته ی **Update**، تغییر در بسته‌های موجود و تغییر در قابلیت‌های نصب شده ی ویندوز مربوط باشد، در این قسمت قابل مشاهده است.

در شبکه‌های بزرگ امروزی با توجه به تعداد زیاد Server ها و نرم‌افزارهای کاربردی و حجم بسیار زیاد Log ها، نظارت روزانه بر همه ی Log ها بدون استفاده از ابزارهای پیشرفته ی Log Monitoring، امکان‌پذیر نیست.

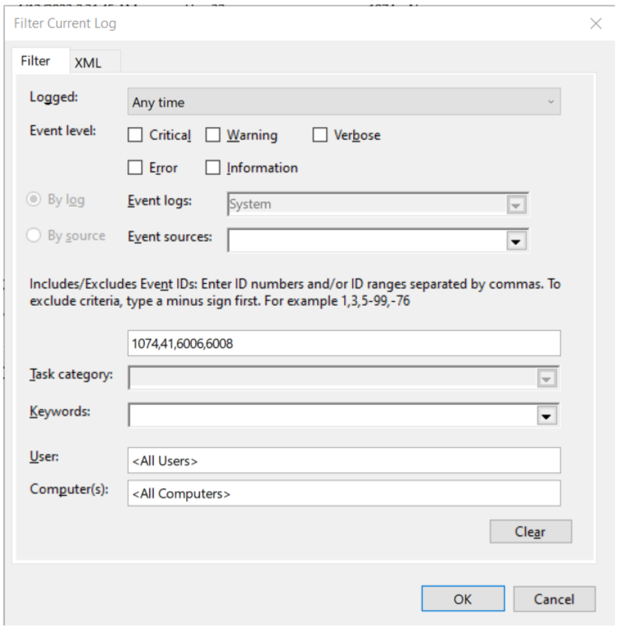
راهنمایی:

- **Event ID : 41** : نشاندهنده ی restart شدن سیستم است، بدون انجام یک Shutdown کامل و سالم.
- **Event ID : 1074** : نشاندهنده ی یک restart یا یک Shutdown، کامل و سالم می باشد.
- **Event ID : 6006** : نشاندهنده ی یک موردخاص از Shutdown است.
- **Event ID : 6008** : نشاندهنده ی یک Shutdown ناخواسته و ناگهانی است؛ که دو حالت دارد:
  - به شکل دستی توسط دکمه ی فیزیکی Restart
  - توسط خود سیستم، پس از دریافت یک پیام خطا و یا عدم تحمل از هنگ شدگی.
- **Event ID : 6005** : نشاندهنده ی این است که event log service روشن می شود، که نشانه ی System Startup است.

می دانیم که گاهی که در حال کار کردن با کامپیوتر، ناگهان یک برنامه سیستم از کار می افتد، به اصطلاح Crash می‌کند.
برای پیدا کردن این Crash ها در سیستم، کافی است:
با روی Application راست کلیک کرده و با انتخاب Find، در کادر محاوره‌ای باز شده عبارت Explorer.exe را وارد کرده و به دنبال تمام رویدادهای مربوط به آن بگردیم؛ که شامل سه نوع Event می باشد. (1000 , 1001 , 1002)

مثال: برای پیدا کردن همه ی event های خاموش شدن کامپیوتر:

System را انتخاب کرده و در کادر سمت راست، Filter Current Log را باز کرده و برای نوار <All Event IDs> به شکل زیر درج کرده و OK:



در PowerShell:

- **برای مشاهده ی مشخصات همه ی Log List ها:**

```
Get-WinEvent -ListLog *
```

دستور سفارشی زیر، واضح تر و بهتر عمل می کند:

```
Get-WinEvent -ListLog * | Select-Object LogName, RecordCount, IsClassicLog, IsEnabled, LogMode, LogType | Sort-Object -Property LogType | Format-Table -AutoSize
```

- **برای مشاهده ی Log List های موجود در یک Server:**

```
Get-WinEvent -ListLog * -ComputerName HOSTNAME
```

- **برای جستجو میان Log List ها، بر اساس نام آنها:**

```
Get-WinEvent -ListLog * | Where-Object LogName -Like "*Cisco*"
```

- **برای دریافت مشخصات کامل یک Log List:**

```
Get-WinEvent -ListLog Security | Format-List -Property *
```

- **برای مشاهده ی Log های موجود در یک Log List:**

```
Get-WinEvent -LogName Security
```

- **برای مشاهده ی Log هایی که در لیست Security و دارای یک Event ID خاص هستند:**

```
Get-EventLog -LogName Security -after 08/29/2023 -Before 09/04/2023 | Where InstanceID -EQ 4624 | Format-Table -AutoSize
```

- **برای مشاهده ی Log هایی که در لیست Application و از نوع Error بوده و در یک بازه ی زمانی مشخص، گزارش شده اند:**

```
Get-EventLog -LogName Application -after 08/31/2023 -Before 09/03/2023 | Where EntryType -EQ Error | Format-Table -AutoSize
```

- **برای export گرفتن از یک Log List دلخواه** (مثلن از Security):

```
wevtutil epl Security F:\TestLogs.evtx
```

Windows Task Schedular:

توسط این کنسول، می توان یک سری فرآیند ها را تنظیم و زمان بندی کرد که به طور خودکار، در زمان های مورد نظر، اجرا شوند.
این فرآیندها می توانند:

- **توسط ابزارهای Windows انجام بگیرند،**
- **توسط نرم افزارهای نصب شده روی Windows انجام بگیرند،**
- **توسط یک سری دستورات به هم پیوسته، که به آن Script گفته می شود، انجام بگیرند.**

این Script ها را هم می توان توسط Command prompt تنظیم کرد، و هم می توان توسط PowerShell نوشت.

- ❖ **آن فرآیند، می تواند ارسال ایمیل، خاموش کردن کامپیوتر، حذف کردن فایل‌های درون یک فولدر موردنظر و ... باشد.**
- ❖ **به هریک از این فرآیند هایی که در این Console تنظیم می شوند تا بطورخودکار اجرا شوند، Task گفته می شود.**

بطورپیشفرض، چند Task در این کنسول تعریف شده اند، مثل update های ویندوز که هر از گاهی بطور خودکار اجرا می شوند.

ایجاد یک Task:

وارد منوی Action شده و گزینه ی Create Basic Task را می زنیم.

- ○ **در تب اول، یک نام و یک توضیح مختصر برای این Task درج می کنیم.**
- ○ **در تب Trigger، می توان فاصله ی زمانی آن را انتخاب کرد و یا اینکه:**
  - **When I log on: با هربار login به سیستم**
  - **When the computer starts : با هر بار روشن شدن کامپیوتر**
  - **When a specific event is logged : در هرزمان که یک log خاص در Event Viewer ایجاد شد.**
- ❖ **در تب Action می توان تعیین کرد که یک برنامه اجرا شود و یا یک اسکریپت اجرا شود.** (ظاهراً بقیه ی موارد غیرفعال هستند!)

مثال:

فرض کنید که بخواهیم محتویات پوشه ی T1 در درایو C، هر یک هفته یکبار، حذف شوند.

- ○ **ابتدا Notepad را باز کرده و متن زیر را در آن کپی می کنیم:**

forfiles /p "C:\Users\NAME\Downloads" /s /m *.* /c "cmd /c Del @path" /d -7

- ○ **اما مسیری که در کد بالا درج شده را به مسیر پوشه ی خودمان در سیستم تغییر می دهیم.**
- ○ **عدد ۷ به معنای تعداد روزهایی است که این فرآیند تکرار خواهد شد.**

نکته: باید دقت کرد که چهار علامت " که در کد وجود دارد، درست درج شده باشند، وگرنه این کد عمل نمی کند.

- ○ **حالا به File و سپس Save As رفته و این فایل ایجاد شده را، به یک نام دلخواه و با پسوند bat. نامگذاری می کنیم.**
- ○ **برای اطمینان از صحت عملکرد این کد، یکبار آن را اجرا و تست می کنیم.**
- ○ **حال در کنسول Task Scheduler وارد ویزارد ایجاد یک Basic Task شده و در تب Action گزینه ی Start a program را زده و توسط Browse آن فایل bat. را وارد می کنیم و تمام!**

نکته: برای مشاهده ی Task هایی که ایجاد کرده ایم، کافی ست در کادر سمت چپ کنسول، فقط پوشه ی Task Scheduler Library را انتخاب کنیم.

نکته: می توان به جهت نظم در کار، از طریق منوی Action و گزینه ی New Folder پوشه یا پوشه هایی را ایجاد کرد و Task های موردنظر را در آنها قرار داد.

مثال:

- **فرض کنید بخواهیم کامپیوتر را در یک زمان خاص به حالت sleep وادار کنیم، کاملاً مشابه با مثال قبل عمل می کنیم، اما با کد زیر:**

Rundll32.exe Powrprof.dll,SetSuspendState Sleep

مثال:

- **فرض کنید بخواهیم در یک زمان خاص، یک ping مدام انجام شود. کاملاً مشابه با روش قبل عمل کرده اما با کد مقابل:**

ping -t 8.8.8.8

مثال:

- **فرض کنید بخواهیم در یک زمان خاص، یک وبسایت باز شود:**
  - **در کنسول Task Scheduler وارد ویزارد ایجاد یک Basic Task شده و در تب Action گزینه ی Start a program را زده و توسط Browse ، فایل اجرایی برنامه ی firefox را که معمولاً در آدرس C:\Program Files\Mozilla Firefox قرار دارد را انتخاب می کنیم.**
  - **در کادر Add arguments آدرس سایت موردنظر را درج می کنیم، مثلاً :** http://www.imdb.com

مثال:

- **فرض کنید بخواهیم کامپیوتر را در یک زمان خاص خاموش کنیم.**
  - **در کنسول Task Scheduler وارد ویزارد ایجاد یک Basic Task شده و در تب Action گزینه ی Start a program را زده و توسط Browse به آدرس** C:\Windows\System32 **رفته و فایل** shutdown.exe **را انتخاب می کنیم.**

- **جهت افزودن یا تغییر تنظیمات Task ها، کافی ست که پس از ایجاد یک Task، روی آن دابل کلیک کرده و تغییرات موردنظر را اعمال کرد.**

گاهی پس از اعمال تغییرات و کلیک بر روی OK با خطایی مشابه missing the required arguments needed to execute the task مواجه می شویم، که باید در تب General گزینه ی Change User or Group را زده و User مدیریتی را انتخاب کرد و سپس سعی در ذخیره ی تغییرات کرد.

برنامه ریزی و اجرای زمانبندی شده ی یک PowerShell Script:

1. **Script ای که توسط PowerShell نوشته شده است را با پسوند PS1. ذخیره می کنیم.**
2. **وارد Task Schedular شده و از کادر سمت چپ، وارد یکی از پوشه های موردنظر می شویم، و یا در همان پوشه/مسیر ش Task Schedular Library کلیک راست کرده و Create Task را می زنیم.**
3. **ابتدا یک نام و یک توضیح در مورد کاری که انجام خواهد شد درج می کنیم.**
4. **وارد تب Trigger شده و بازه ی زمانی موردنظر را تنظیم می کنیم.**
5. **وارد تب Action شده و New Action را زده و برای Program/Script آدرس فایل اجرایی PowerShell را در سیستم درج می کنیم:**

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

6. **برای نوار Add arguments، آدرس Script ای که نوشته و ذخیره کرده ایم را به صورت زیر درج می کنیم:**

-WindowStyle Maximized -command "C:\...\NameOfData.ps1"

Safe mode :

وقتی در حالت معمولی، سیستم را روشن می کنیم و وارد ویندوز و **Account** خود می شویم، در حقیقت در یک حالت معمولی و استاندارد وارد شده ایم که همه ی **Service** ها و درایورها و نرم افزارهایی که تعیین کرده بوده ایم، بطور خودکار فعال و روشن هستند؛ به این حالت **Standard start up** گفته می شود.

Safe mode هم، یک نوع **start up mode** می باشد: **Safe mode start up**

وضعیتی است، که سیستم عامل را بالا می آوریم، همه چیز سر جایش است، اما:

- بیشتر **Service** ها و بیشتر **Driver** ها، خاموش و غیرفعال هستند.
- سرویس‌ها و امکانات داخلی سیستم عامل، محدود به موارد ضروری می‌شوند.

وضعیت **Safe mode**، مزایای ارزشمندی دارد، مثلاً:

- در این حالت، به سادگی می توان سعی در رفع مشکلات ناشی از نرم‌افزارها کرد.
- به سادگی می توان **Driver** به روزرسانی شده ای که ایجاد مشکل کرده بوده است را، به نسخه ی قبلی که بدون مشکل کار می‌کرده است، بازگرداند، یا به قولی، **roll back** کرد.

خود وضعیت **Safe mode** دارای دو حالت می باشد:

- **Safe mode**
- **Safe mode with networking**

این دو حالت خیلی مشابه یکدیگر هستند، اما در حالت **networking**، سرویس های **network** و **Internet** بطور استثنا، همچنان برقرار و روشن هستند، تا بتوان ارتباط با اینترنت و یا سیستمهای دیگر عضو شبکه را همچنان داشت.

رفع عیب در Safe mode:

❖ فرض کنید یک سیستم دچار ویروس یا بدافزار شده است.
می دانیم که بیشتر بدافزارها در حالت طبیعیِ ویندوز، قابل از بین بردن نیستند، چون در **Background** در حال اجرا هستند و در کار آنتی‌ویروس نیز خلل ایجاد می‌کنند.
پس وارد **safe mode** شده و آنتی‌ویروس را اجرا می کنیم تا به سادگی بدافزار را از بین ببرد؛ و یا اگر **Antivirus** نداشته باشیم، می توانیم در همان حالت **safe mode** یکی را دانلود و نصب و اجرا کنیم؛ و یا اینکه در ویندوز **10**، در همان **safe mode**، نرم افزار **windows defender** را باز کرده و **Scan offline** را اجرا می کنیم.

❖ فرض کنید که سیستم شما بطور ناگهانی دچار مشکل شده است و بالا نمی آید.
پس وارد **safe mode** شده و به سادگی توسط **System Restore**، سیستم را به زمانی که ویندوز بدون مشکل کار می‌کرده برگردانید.

❖ فرض کنید اخیرا نرم‌افزاری را نصب کرده‌اید که باعث می‌شود سیستم بطورمرتب با ایراد صفحه آبی (**BSoD**) روبرو شود. پس وارد **safe mode** شده و از طریق **Control panel** آن نرم‌افزار را پاک می کنیم.

❖ فرض کنید ویندوز در حالت طبیعی ثبات ندارد، ولی در **Safe mode** به‌درستی کار می‌کند، پس به احتمال زیاد یکی از نرم‌افزارها دردسرساز شده است، که آن را در **Safe mode** حذف می کنیم.
اما اگر در **Safe Mode** هم، ویندوز ثبات ندارد، احتمال وجود یک مشکل سخت‌افزاری در سیستم وجود دارد.

- ❖ فرض کنید سیستم عامل **update** شده، اما حالا دیگر بالا نمی آید.
- ❖ باید وارد **safe mode** شده و **update** ها را برگرداند یا **roll back** کرد:

Settings > Update & Security > View Update History and click the Uninstall Updates link

- ❖ فرض کنید یک **Remote user** اعلام می کند که سیستمش دچار یک آلودگی یا مشکل نرم افزاری شده است.

پس نیاز است که یک **remote connection** با او برقرار کنیم.

اما قبل از آن، باید ابتدا از او بخواهیم وارد **safe mode with networking** شود، و سپس توسط **remote connection** به او متصل شویم.

ورود به Safe mode**:**

در سیستم های قدیمی تر، می توان یکبار سیستم را **restart** کرد و با فشردن دکمه ی **F8** و یا **Shift+F8** در هنگام **Boot**، گزینه ی **Safe Mode** را انتخاب کرده و وارد سیستم عامل شد.

اما در سیستم های **UEFI** و یا سیستم هایی که سیستم عامل شان بر روی **SSD** نصب شده است، نمی توان به این شکل وارد تنظیمات **Start up Mode** شد. پس در خود سیستم عامل ویندوز:

- ابتدا پنجره ی **System Configuration** را باز می کنیم. (در **Run** درج می کنیم: msconfig)
- در تب **Boot** گزینه ی **Safe Boot** و سپس **minimal** را فعال و **Apply** می کنیم.
- سپس در تب **General** می بینیم که **Selective Startup** انتخاب شده است، کافی ست که از زیرگزینه های آن، فقط گزینه ی **load startup items** را فعال کنیم. **OK** می کنیم و **Restart**.

:Windows Installation

- همانطور که می دانیم، می توان از طریق رسانه های مختلف، سیستم عامل را روی سیستم نصب کرد:
  USB، **optical drive**، **Network** و .... اما سریع ترین روش، از طریق **USB** خواهد بود.
- برای به روزرسانی کامل یا نصب مجدد **Windows**، طوری که تمامی تنظیمات و فایل های موجود، باقی و بی تغییر بمانند، و نیازی به نصب مجدد برنامه ها نباشد، از نصب **RU** یا همان **refresh upgrade** استفاده می کنیم، که به آن **in-place upgrade** هم گفته می شود.
- برای **repair** کردن ویندوز، پس از دابل کلیک کردن روی فایل نصب یا اجرا کردن **Autorun** مربوط به فایل نصب، بر روی **Install now** کلیک کرده و گزینه ی **upgrade** را می زنیم و نه **Advanced** (**custom**).

➢ :Image deployment

فرض کنید بخواهیم مثلاً برای **5** کامپیوتر:

- یک ویندوز **10** نصب کنیم.
- **Firefox** را نصب و **Internet explorer** را غیرفعال کنیم.
- **Adobe Photoshop** و **Microsoft Office** را نصب کنیم.

خب ما می توانیم، یک **Image** از فایل نصب ویندوز تهیه کنیم، و این **Image** را طوری تنظیم کنیم که این سفارشی سازی های **Firefox** و **IE** و **office** و **photoshop** را نیز به آن اضافه کرده باشیم.

سپس کافی ست این **Image** ساخته شده را روی هریک از **5** کامپیوتر نصب کنیم. بطورخودکار همه ی عملیات مدنظر، روی همه ی آنها، انجام خواهد گرفت.

به این روش، **Image deployment** گفته می شود.

اما نصبِ ویندوز به شکل **Image deployment** کاملاً خودکار پیش نمی رود، و باید در صورت نیاز به تنظیمات زبان یا انتخاب درایو نصب و ...، آنها را بصورت دستی پیش ببریم.

➢ :unattended installation

این مدل نصب ویندوز، خواه ناخواه **Image deployment** می باشد.

اگر بخواهیم نصب ویندوز، کاملاً خودکار و یکسره پیش برود، طوری که در پایان، ویندوز نصب و کامل و آماده ی **Login** شدن باشد، یک فایل طراحی می کنیم که به آن **Answer file** گفته می شود، که برای همه ی تنظیمات و **Wizard** های که ظاهر خواهند شد، یک گزینه را در این فایل **Answer** تنظیم می کنیم و این فایل را مشابه با **Image deployment** به فایل نصب ویندوز ضمیمه می کنیم.

سپس پس از آغاز فرآیند نصب، دیگر نیاز به هیچگونه دخالت و دستکاری ما نمی باشد، و تمامی مراحل نصب، تا پایان به شکل خودکار پیش می روند.

نصب ویندوز به صورت **unattended**، سریع ترین روش نصب ویندوز می باشد.

Windows Registry :

تنظیمات اولیه ی اتصال یک سخت افزار و یا نصب یک نرم افزار بر روی سیستم، در یک بانک داده ی سلسله مراتبی (hierarchical database) در ویندوز ذخیره می شوند، که **Registry** نام دارد.

Linux روش ساده‌تری را استفاده می کند و این تنظیمات را درون فایل‌ها ذخیره می‌کند. که البته برای کسی که می خواهد روی این تنظیمات کار کند، کمی پیچیده تر خواهد بود.

مشکل این روش، گستردگی و غیرمتمرکز بودن فایل‌هاست و کاربر مجبور می شود که برای پیدا کردن هر فایل و روش تنظیمات آن، تخصص بالایی داشته باشد!

Microsoft روش سخت‌تری را برای خودش انتخاب کرده است که البته کار برای کاربر ساده‌تر خواهد بود.

Registry یک پایگاه داده ی پیشرفته است که امکانات زیادی دارد.

هر گونه تغییر در پیکربندی سخت یا نرم افزار، در **Registry** هم اعمال خواهد شد.

همچنین **Windows Registry** دسترسی مستقیم به مقدار زیادی از اطلاعات دارد:

- پروفایل همه ی **Account** های کاربران
- اطلاعات در مورد هریک از برنامه های نصب شده
- انواع فایل هایی که می توانند توسط هر برنامه ایجاد شوند.
- اطلاعات مربوط به ویژگی های **Folder** ها و **Shortcut** های برنامه ها
- پورت هایی که هریک از سخت افزارهای نصب شده استفاده می کنند.

نکته: همه ی **Software** ها، از **Registry** استفاده نمی کنند. برخی از آنها پیکربندی های خود را در یک فایل **XML** ذخیره می کنند، و یا مثلاً برنامه های **Portable**، پیکربندی های خود را در فایل های اجرایی شان ذخیره می کنند.

اینکه چه زمانی به تنظیمات **Registry** مراجعه می کنیم یا نیاز پیدا خواهیم کرد، یک روند ساده دارد:

- اگر مشکلی در ویندوز از طریق **Control Panel** یا گزینه های موجود در صفحه ی **Settings** حل و رفع نشد؛ به **cmd** می رویم.
- اگر مشکل موردنظر، از طرق **cmd** هم رفع نشد، به **PowerShell** می رویم.
- اگر از طریق **PowerShell** هم رفع نشد، به کنسول **Registry Editor** می رویم.

برای دسترسی به این بانک، کافی ست در خط فرمان **RUN** درج کنید: **regedit**

هر نسخه از **Windows**، شامل نسخه ی منحصر به فرد از رجیستری است.

Registry از چندین فایل مختلف تشکیل‌شده است. این فایل‌ها از نوع **Binary** هستند و محل نگهداری آنها در مسیر زیر است:

%systemroot%\system32\config

برخی از فایل های مهم آن:

- **SAM** (**Security Account Manager**):

شامل همه ی اطلاعات مربوط به **Account** های تعریف شده روی سیستم جاری (**local machine**) را شامل می شود.

- **SECURITY**:

شامل همه ی تنظیمات و **policy** ها و **permission** های مربوط به یک **User** و نرم افزارهای مورداستفاده اش است.

- **SOFTWARE**:

شامل همه ی تنظیمات مربوط به نرم افزارهاست.

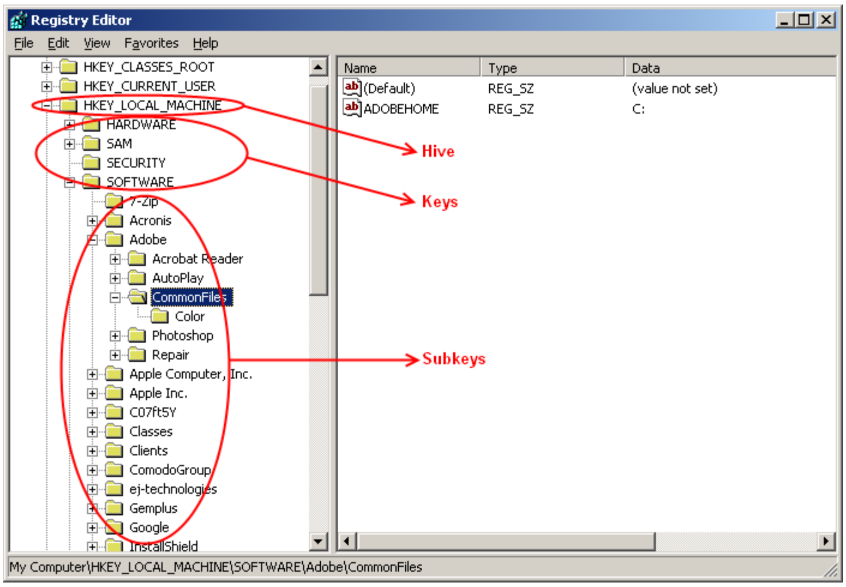
- **SYSTEM**:

شامل همه ی اطلاعات مربوط به تنظیمات پیشفرض سخت افزارهای متصل و درایورهای آنهاست.

نکته: البته فایل های مهم دیگری نیز برای پایگاه داده ی Registry وجود دارند که مکان آنها در جای دیگری است.

➢ Structure:

با وارد شدن به کنسول رجیستری، Folder های اصلی که در پانل سمت راست مشاهده می کنید، با نام **Hive** یا کَندو، شناخته می شوند.
درحقیقت ساختار Registry به شکل درختواره یا Tree است که Hive ها، ریشه ها یا Root های آن هستند.
هر Hive دارای تعدادی Key است و هر Key شامل زیر پوشه هایی می باشد که Subkey نامیده می شوند.
تعداد Hive ها ثابت است، نه می توان یکی را حذف کرد و نه می توان اضافه کرد.



در رجیستری، 5 نوع Hive داریم:

HKEY_CLASSES_ROOT (HKCR):

- تنظیمات نرم افزاری مربوط به File System
- اطلاعات مربوط فرمت فایل های مختلف
- اطلاعات میانبر(shortcut information)
- اطلاعات در مورد File associations: بطوراساسی توسط ویندوز برای استفاده از برنامه ها می باشد.

و سایر رابطهای کاربری در این Hive ذخیره می شوند.

HKEY_CURRENT_USER (HKCU):

تنظیمات پیکربندی برای هر Item سخت افزاری و نرم افزاری مربوط به هریک از User Account های سیستم جاری
این Hive بصورت داینامیک است. یعنی هر کاربر که به سیستم Log in کند، تنظیمات مربوط به او، از Subkey مربوطه اش در HKEY_USERS، به عنوان پروفایلش، بازیابی شده و در این Hive نیز ذخیره می شوند.

HKEY_LOCAL_MACHINE (HKLM):

تنظیمات پیکربندی سخت افزار و نرم افزار برای همه ی User ها، در این Hive ذخیره می شوند.
یعنی دیگر فرقی ندارد که چه کاربری پشت این سیستم بصورت interactive نشسته و login می کند. تنظیمات این Hive برای همه ی کاربران اعمال خواهد شد.

HKEY_USERS (HKU):

- شامل تنظیمات پیکربندی برای هر Item سخت افزاری و نرم افزاری مربوط به هریک از User Account های سیستم جاری است.
- اطلاعات موجود در پوشه های کاربر
- انتخاب Theme های کاربر
- رنگ ها و تنظیمات Control Panel به عنوان پروفایل کاربر ذخیره می شوند.

این hive دارای یک subkey به ازای هر User Profile است.

: HKEY_CURRENT_CONFIG

تنظیمات کنونی سخت افزار سیستم، اشاره به HKEY_LOCAL_MACHINEConfig در این Hive ذخیره می شوند.
این hive هم بصورت dynamic است. به این معنی که در زمان اجرا، ساخته می شود.

➢ :Backup

همیشه قبل از اعمال حتی کوچکترین تغییرات، بهتر است که یک Backup از Registry تهیه کنیم.

برای ایجاد یک نسخه ی Backup از تمام تنظیمات Registry کافی ست روی آیکون کامپیوتر آن کلیک راست کرده و Export را بزنیم.
برای بازیابی این فایل Backup، کافی ست از منوی بالا، File و Import را بزنیم.
درحقیقت این فایل Backup، یک فایل با پسوند reg. می باشد.
درحقیقت این فایل reg. چیزی بیش از یک فایل ساده ی متنی نیست، که دستورالعملهایی برای ابزار regedit برای اضافه کردن، تغییر و یا حذف Key در رجیستری، بدون هرگونه اشتباه تصادفی است.
می توان این فایل را با کلیک راست و گزینه ی Edit، توسط Notepad نیز مشاهده و ویرایش کرد.
می دانیم که هر گونه تغییر و تنظیم اشتباه در رجیستری، ممکن است پیامدش سقوط سیستم باشد.
اگر شما تنظیمات نرم افزاری مثل SQL Server یا Office را در سیستم تان به هم بریزید، این دستکاری فقط شامل همان نرم افزار خواهد شد؛ اما چون رجیستری، پایگاه داده ی تمام ویندوز است، می تواند منجر به صغوط سیستم شود.
یک مزیت فایل های آماده ی reg. این است که خطای انسانی را به شدت کاهش داده و فقط تغییراتی که در مسیر خاصی از رجیستری باید رخ دهند را در رجیستری اعمال می کنند.

➢ :Defragmentation

همانطور که در زمان کُندی و یا جهت جلوگیری از کُندیِ حافظه های HDD آنها را defrag می کنند، برای بهبود کُندی و یا جلوگیری از آن، Windows Registry را هم defragment می کنند.
که توسط ابزارهای رایگانی همچون ابزارهای زیر، قابل defragmentation می باشد:

Free Registry Defrag
Registrar Registry Manager Lite
Registry Compressor
WinUtilities Registry Defrag
Eusing Free Registry Defrag
NTREGOPT
PageDefrag

:Values ⮚

برای هر یک تغییر در **Registry**، باید یک مقدار (**Value**) جدید در آن تعریف شود و یا یکی از مقادیر موجود تغییر کند.
یک **key** یا **subkey** می تواند حاوی یک یا چند **Value** و البته یک **default value** باشد.
هر **Value** همیشه دارای سه ویژگی می باشد:

Name ،Data Type ،value data

مثلاً

[0x8000000] [REG_DWORD] [RegistrySizeLimit]

پس **Registry** شامل انواع مختلفی **Value** است، که در **11** حالت دسته بندی می شوند:

Name	Data type
REG_BINARY	Binary
REG_DWORD	Numeric
REG_QWORD	Numeric
REG_EXPAND_SZ	String
REG_FULL_RESOURCE_DESCRIPTOR	String
REG_LINK	String
REG_MULTI_SZ	Multi-string
REG_NONE	Unknown
REG_RESOURCE_LIST	String
REG_RESOURCE_REQUIREMENTS_LIST	String
REG_SZ	String

Value های حجیم (بیش از **2048** بایت) در **external file** ذخیره می شوند و نام آن فایل به رجیستری اضافه می شود.
این باعث می شود که **Registry** کارآمدتر ظاهر شده و به کار خود ادامه دهد.

➢ Data Type :

REG_BINARY :

مقادیر باینری، در یکی از دو حالت صفر و یک قرار خواهند داشت؛ که صفر به معنی خاموش یا غیرفعال بودن و یک به معنی روشن یا فعال بودن است.

بیشتر اطلاعات مربوط به دستگاه های سخت افزاری، در قالب داده های باینری ذخیره می شوند و به شکل **Hexa decimal** در ویرایشگر **Registry** نمایش داده می شوند.

REG_DWORD :

داده ها به عنوان یک عدد صحیح 32 بیتی(**Integer**) (4 بایتی) و در فرمت **Binary** یا **Hexa decimal** و یا اعشاری نمایش داده می شوند.

بسیاری از **Service** ها و بسیاری پارامترهای **Driver** های دستگاه ها، دارای این نوع هستند.

این مقدار برای سیستم‌عامل‌های 32 بیتی طراحی‌شده است، ولی در سیستم‌عامل‌های 64 بیتی نیز استفاده می‌شود.

REG_QWORD :

مشابه مقدار **DWORD** است، که البته برای سیستم عامل های 64 بیتی طراحی شده است و برای سیستم های 32 بیتی بکار نمی آید.

REG_SZ (String):

یک رشته متن کوتاه در یک فرمت مناسب، برای ادراک انسان هاست. به این معنی که این رشته، یک متنِ کوتاه است که می تواند در یک فراخوانی یا **Call** از یک برنامه، جایگزین شود. مثل مسیر پوشه ها و فایل ها.

مقدار آن را می توان به سادگی تغییر داد.

REG_MULTI_SZ:

با توجه به اینکه در نوع **String**، مقدار رشته ی قابل استفاده، کوتاه بود، مقدار **multi-string** یا مقدار چند رشته ای، طراحی شد که می تواند قادر به ذخیره ی چند خط اطلاعات متنی یا همان لیستی از **String** ها باشد.

این رشته ها با **Space** و یا **comma** یا سایر نمادها جدا می شوند.

REG_EXPAND_SZ (Expandable String):

همانطور که می دانیم، در برنامه نویسی با متغیرها سر و کار داریم، اگر بخواهیم درون یک **Value**، از یک متغیر استفاده کنیم، دیگر نوع داده ی **String** کارآمد نیست. پس از این مقدار استفاده می کنیم که قادر به ذخیره‌سازی متغیرهای محیطی است.

REG_LINK :

یک لینک نمادین یا **Symbolic** در **Unicode** است.

REG_FULL_RESOURCE_DESCRIPTOR :

مجموعه ای از آرایه های تو در تو است.

این ذخیره ای از لیست **Resource** هاست که توسط یک **Hardware** استفاده می شوند.

سیستم، داده های شناسایی شده را برای درختواره یا **tree** مربوط به **HardwareDescription** می نویسد.

در **editor**، این داده ها به عنوان یک مقدار باینری در فرمت هگزادسیمال نمایش داده می شود.

REG_RESOURCE_LIST :

مجموعه ای از آرایه های تو در تو هستند. این یک لیست منابع استفاده شده توسط یک درایور دستگاه یا یک دستگاه سخت افزاری که توسط آن درایور کنترل می شود را ذخیره می کند.

سیستم دادههای کشف شده را در درختواره ی ResourceMap می نویسد.

در ویرایشگر، این داده ها به عنوان یک مقدار باینری در فرمت هگزادسیمال نمایش داده می شوند.

REG_RESOURCE_REQUIREMENTS_LIST :

مجموعه ای از آرایه های تو در تو هستند.

این مورد برای ذخیره ی لیستی از درایور های سخت افزاری استفاده می شود که می تواند توسط یک درایور دستگاه خاص یا دستگاهی که توسط آن درایور کنترل می شود، استفاده شود.

در ویرایشگر، داده ها به عنوان یک پارامتر باینری در فرمت هگزادسیمال نمایش داده می شوند.

REG_NONE :

هیچ داده ای در یک key ذخیره نمی شود.

داده ها توسط سیستم یا یک برنامه در Registry نوشته می شوند.

در ویرایشگر یاEditor ، به عنوان یک مقدار باینری در فرمت هگزادسیمال نمایش داده می شود.

➢ Key or Value:

بطور مثال، به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\

جهت ایجاد Key یا Value:

روی همان پوشه ی Policies کلیک راست کرده و New و سپس Key را می زنیم و یک نام (بر اساس سند یا Document موردنظر) درج می کنیم.

جهت ایجاد یک Value، کافی در همان کلیک راستی که کردیم، یکی از value type ها را انتخاب کرده و سپس یک نام موردنظر تعیین کنیم.

جستجوی Key ها و Value ها:

فرض کنید یک Key یا یک Value ایجاد کرده باشید و پس از مدتی، مکان ایجاد آن را فراموش کرده باشید و به قسمتی که navigate می کنید، آن را پیدا نمی کنید!

پس توسط ابزار Find در کنسول Registry اقدام می کنید، که با دکمه ی F3 و یا در منوی Tools و گزینه ی Find قابل فراخوانی است.

به سادگی می توان هرگونه Key، Value و یا Data را جستجو کرد.

اگر قصد جستجوی اطلاعات بیشتری در Registry را داشته باشیم، می توان از یکی از دو نرم افزار رایگان زیر استفاده کرد:

- RegScanner
- Registry Finder

توسط آنها می توان از نتیجه ی جستجو نیز یک export تهیه کرد.

➢ Registry Tricks:

فرض کنید، بخواهید تمام تنظیمات موجود در **Registry** را ذخیره کرده و در یک سیستم دیگر، این تنظیمات را **Import** کنید:

- کافی ست که از منوی بالای کنسول **Registry** گزینه ی **File** و سپس **Export** را زده و آن را با پسوند **reg.** ذخیره کنیم.
- حال در هر کامپیوتری که روی این فایل ذخیره شده دابل کلیک و **OK** کنیم، آن تغییر بطور سریع اعمال می شود و نیازی به ورود به **Key** ها و **Value** های **Registry** سیستم مقصد و تغییر دستی آنها نیست.

فرض کنید فقط در یکی از **Value** های **Registry** سیستم، تنها یک عدد را تغییر داده اید. حال قصد دارید، این تغییر را در سیستم های دیگر نیز اعمال کنید:

- کافی ست که روی همان **Hive** یا حتی فقط روی همان **Key** مربوطه، کلیک راست کرده و **Export** را بزنیم و آن را با پسوند **reg.** ذخیره کنیم.
- حال در هر کامپیوتری که روی این فایل ذخیره شده دابل کلیک و **OK** کنیم، آن تغییر بطور سریع اعمال می شود و نیازی به ورود به **Key** ها و **Value** های **Registry** سیستم مقصد و تغییر دستی آنها نیست.

نکته: همیشه برای کار با **Registry** تا جای ممکن لازم است که آن را با دسترسی **Administrator** باز کنیم.

نکته: وقتی یک فایل **Reg.** را اجرا می کنیم، تمام تنظیمات آن، جایگزین تمام تنظیمات جاری **Registry** می شود.
یعنی اگر در فایل **Reg.** مقدار یک **value**، خالی باشد. اما در تنظیمات جاری **Registry** مقدار آن برابر با یک عدد باشد.
پس از اجرای فایل **reg.**، مقدار آن **value** نیز خالی خواهد شد.

نکته: گاهی ممکن است که از چند **Key** یا یکی دو **Hive** مختلف، **export** هایی تهیه کرده باشیم، و حال بخواهیم این فایل های **export** شده را **merge** و یکی کنیم.
نرم افزارهایی وجود دارند که این کار را انجام می دهند، مثل RegFileMerger

Show the windows version :

می دانیم که با وارد کردن دستور **winver** در **RUN** ، پنجره ای باز شده و ورژن و مشخصات کلی ویندوز را نشان می دهد.
اما جهت درج دائمی ورژن ویندوز بر روی **Desktop**، به مسیر زیر می رویم:

HKEY_CURRENT_USER\Control Panel\Desktop

مقدار **PaintDesktopVersion** را پیدا کرده و با دابل کلیک وارد تنظیمات آن شده و **Value data** آن را از **0** به **1** تغییر می دهیم و **OK**.

Prevention of background image change :

البته این کار را می توان از طریق **Group policy** ها هم انجام داد؛ اما در **Registry** به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

- روی **Policies** کلیک راست کرده و با انتخاب **New** ، گزینه ی **Key** را انتخاب می کنیم.
- نام این **Key** را **ActiveDesktop** قرار داده و آن را انتخاب می کنیم و در کادر روبرو و در یک فضای خالی، کلیک راست کرده و از **New** گزینه ی **DWORD (32-bit) Value** را انتخاب می کنیم.
- نام این **Value** را **NoChangingWallPaper** قرار داده و وارد **Properties** آن شده و **Value data** را از **0** به **1** تغییر داده و **OK** می کنیم.

حال کاربران قادر به تنظیم یک تصویر جدید برای پس زمینه نخواهند بود و گزینه ی **Set as desktop background** کار نخواهد کرد.

: Set a mandatory background image

به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

- روی **Policies** کلیک راست کرده و با انتخاب **New** ، گزینه ی **Key** را انتخاب می کنیم.
- نام این **Key** را **System** قرار داده و آن را انتخاب می کنیم و در کادر روبرو و در یک فضای خالی، کلیک راست کرده و از **New** گزینه ی **String value** را انتخاب می کنیم.
- نام این **Value** را **Wallpaper** قرار داده و وارد **Properties** آن شده و برای **Value data** آدرس دقیق (همراه با نام و فرمت) تصویر موردنظر را وارد می کنیم و **OK**.

در حقیقت جهت اینکه علاوه بر انتخاب یک تصویر به عنوان پیشفرض غیرقابل تغییر، می توانیم **wallpaper style** یا نوع قرار گیری آن در **Background** را نیز مشخص کنیم. پس:

- در همین مسیر، دوباره کلیک راست کرده و از **New** گزینه ی **String value** را انتخاب می کنیم.
- نام این **Value** را **WallpaperStyle** قرار داده و وارد **Properties** آن شده و برای **Value data** یکی از مقادیر زیر را وارد کرده و **OK** :

0 - Centered
1 - Tiled
2 - Stretched
3 - Fit
4 - Fill

:Prevention the word "Shortcut"

همانطور که می دانیم، وقتی روی آیکون اجرایی یک نرم افزار، **Create Shortcut** را می زنیم، یک نسخه ی میانبور از آن ایجاد می کند، اما کلمه ی **Shortcut** را به نام آن نسخه ی جدید اضافه می کند!

- برای حذف این کلمه، به مسیر زیر می رویم:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- سپس در اینجا باید **BINARY value** ای به نام **link** را بیابید. اگر آن را نمی یابید، باید خودتان آن را ایجاد کنید!
- وارد تنظیمات **Properties** این مقدار می شویم.
- مقدار **00 00 00 00** را در **Value data** آن وارد می کنیم و **OK**!
- پس از اعمال این تنظیمات لازم است که یک بار از سیستم **Sign out** کرده و از نوع **Sign in** کنیم.

:Disable the right click and disappear Desktop icons

به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

نکته: اگر **Key** یا پوشه ی مربوط به **Explorer** در این مسیر وجود نداشت، خودمان دستی آن را ایجاد می کنیم.

اگر در کادر سمت راست، مقداری به نام **NoDesktop** و از نوع **DWORD (32 bit)** وجود ندارد، آن را نیز دستی ایجاد می کنیم.

با دابل کلیک کردن روی **NoDesktop** وارد تنظیمات آن شده و مقدار **value data** را به عدد یک تغییر می دهیم.

حال اگر یکبار سیستم را **Restart** کنیم یا **sign out** و از نو **sign in** کنیم، متوجه ناپدیدشدن آیکون های **Desktop** و غیرفعال شدن کلیک راست خواهیم شد.

برای بازگرداندن به حال اول، به بهمان مسیر در **Registry** رفته و مقدار **value data** را به عدد صفر تغییر می دهیم.

: Remove small arrow on the shortcut icons

به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- حال روی همین پوشه ی **Explorer** کلیک راست کرده و **New** و **Key** را زده و نام آن را **Shell Icons** قرار می دهیم.
- حال، **Shell Icons** را انتخاب کرده و در سمت راست، در یک فضای خالی، کلیک راست کرده و از منوی **NEW** گزینه ی **String Value**را زده و نام آن را عدد **29** قرار می دهیم.
- با دابل کلیک روی **29**، وارد تنظیماتش شده و در قسمت **Value data**، مقدار زیر را وارد کرده و **OK** می کنیم:

%windir%\System32\shell32.dll,-50

- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappear the Shutdown, Restart and Hiberate buttons

این قاعده زمانی به کار می آید که تصمیم داشته باشیم کامپیوترها را از **Shutdown** شدن، **Restart** و یا **Hibernate** شدنِ ناگهانی، مصون نگاه داریم؛ پس به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- **Explorer** را انتخاب کرده و در سمت راست، در فضای خالی، کلیک راست کرده و از**New** ، گزینه ی **32-bit DWORD value** را انتخاب می کنیم.
- نام این **DWORD** را **NoClose** تنظیم می کنیم.
- با دابل کلیک روی **NoClose** به پنجره ی تنظیمات آن وارد شده و **Value data** را که بصورت پیشفرض عدد **0** است، به عدد **1** تغییر می دهیم و تمام!

برای برگرداندن وضعیت به حالت قبل، کافیست که **Noclose** را حذف کنیم.

: Hide the My Computer/This PC Icon from desktop

به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum

اگر **Key** یا پوشه ی **NonEnum** در این مسیر وجود ندارد، باید خودمان دستی آن را ایجاد کنیم.

سپس **NonEnum** را انتخاب کرده و در فضای خالی مقابل، کلیک راست کرده و از **New** گزینه ی **DWORD (32 bit)** را انتخاب می کنیم.

- نام آن را عبارت زیر قرار می دهیم:

{20D04FE0-3AEA-1069-A2D8-08002B30309D}

- روی آن دابل کلیک می کنیم تا پنجره تنظیمات باز شده و سپس **value data** را که بصورت پیش فرض عدد **0** است، به **1** تغییر داده و پنجره را **OK** می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

: Welcoming text on windows Login page

به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/Policies/System/

- روی **Value** مربوط به **legalnoticecaption** دابل کلیک کرده و در قسمت **Value data** عنوان پیغام را درج می کنیم و **OK**.
- حال روی **Value** مربوط به **legalnoticetext** دابل کلیک کرده و در قسمت **Value data** متن پیغام را درج می کنیم و **OK**.
- حال پیغام تنظیم شده، پیش از **Login** به ویندوز، نمایش داده خواهد شد.

: change the windows Login screen picture

توسط Registry می توانیم آن را غیرفعال کنیم:

به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System

- روی خود پوشه ی System کلیک راست کرده و NEW و Value (32-bit) DWORD را زده و نام آن را DisableLogonBackgroundImage قرار می دهیم.
- روی این آبجکت کلیک راست کرده و Modify را می زنیم.
- مقدار Value data آن را از صفر به یک تغییر داده و OK را می زنیم.

توسط کنسول Edit Group Policy می توانیم آن را تغییر دهیم:

- به مسیر زیر می رویم:

Computer Configurations > Administrative Templates > Control panel > Personalization

- در سمت راست، گزینه ی Force a specific default lock screen and logon image را باز می کنیم.
- آن را Enabled کرده و در پایین، آدرس تصویر موردنظر را وارد می کنیم.

: Remove the Manage-option by right click on This PC

به مسیر زیر می رویم:

HKEY_CURRENT_USER/Software/Microsoft/Windows/Current Version/Policies/Explorer/

- وارد تنظیمات Value مربوط به NoManageMyComputerVerb می شویم. اگر این Value وجود ندارد، در فضای خالی مقابل، کلیک راست کرده و از New گزینه ی DWORD (32 bit) را انتخاب می کنیم.
- نام آن را عبارت زیر قرار می دهیم: NoManageMyComputerVerb
- مقدار این Value بصورت پیشفرض 0 است و در این حالت گزینه Manage همچنان فعال است. شما باید روی همین Value دابل کلیک کنید تا وارد پنجره Properties آن شده و Value data را از عدد 0 به عدد 1 تغییر دهید.

: Remove the Properties-option by right click on This PC

توسط این ترفند، علاوه بر حذف شدن گزینه ی Properties در راست کلیک روی This PC، همچنین دیگر با انتخاب This PC و فشردن Alt+Enter نیز، به صفحه ی System هدایت نخواهیم شد.

به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- وارد تنظیمات Value مربوط به NoPropertiesMyComputer می شویم. اگر این Value وجود ندارد، در فضای خالی مقابل، کلیک راست کرده و از New گزینه ی DWORD (32 bit) را انتخاب می کنیم.
- نام آن را عبارت زیر قرار می دهیم: NoPropertiesMyComputer
- حالا روی NoPropertiesMyComputer دابل کلیک کرده و وارد پنجره ی Properties آن شده و مقدار Value data را از 0 به عدد 1 تغییر می دهیم و OK.
- حال فقط کافیست یکبار سیستم را Sign Out کرده و دوباره Sign in کنیم.

: Remove the Properties-option by right click on Recycle bin

به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- **Value** ی **NoPropertiesRecycleBin** را پیدا می کنیم.
- اگر این **Value** در این مسیر موجود نبود، آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- سپس روی این **Value** دابل کلیک کرده و **Value data** را از عدد **0** به عدد **1** تغییر می دهیم و **OK**.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Add Control Panel to right click menu

به مسیر زیر می رویم:

HKEY_CLASSES_ROOT\Directory\Background\shell

حال در زیر **Shell** یک **subkey** ایجاد می کنیم به نام **Control Panel**. (در واقع این نامی است که در **Context menu** (کلیک راست) نمایش داده خواهد شد.

- در زیر **Control Panel** هم یک **Key** جدید ایجاد می کنیم به نام **Command**.
- **Command** را انتخاب کرده و از پنجره ی مقابل، روی **Value** ی **Default** دابل کلیک کرده و سپس برای **Value data**، مقدار زیر را درج می کنیم:

rundll32.exe shell32.dll,Control_RunDLL

- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Disable the context menu in desktop

جهت غیرفعال کردن کلیک راست در صفحه ی **desktop**، به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- **Value** ی **NoViewContextMenu** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **NoViewContextMenu** دابل کلیک کرده و در تنظیمات آن، **value data** را از صفر به یک تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Speed change of menus appearance

این تغییر در کل سیستم تاثیر خواهد داشت و سرعت نمایش منوها را در ویندوز بالا می برد.

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Control Panel\Desktop

- وارد تنظیمات **value** ی **MenuShowDelay** شده و می بینیم که مقدار **Value data** که بر حسب میلی ثانیه است، بر روی **400** قرار دارد؛ پس آن را بطورمثال بر روی **100** قرار داده و **OK**.

نکته: زیاد جالب نیست که این عدد را به صفر برسانیم، چون **menu** ها آنقدر سریع ظاهر می شوند که استفاده از آنها را سخت تر می کند.

- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Folder Option

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- **Value** ی **NoFolderOptions** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **NoFolderOptions** دابل کلیک کرده و در تنظیمات آن، **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Prevent to connect and access the Removable storages

- برای بستن این قابلیت برای یک کاربر خاص، به مسیر زیر می رویم:

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

- برای بستن این قابلیت برای هر کاربری که به این سیستم وارد می شود، به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

- اگر در هریک از مسیرهای بالا، پوشه ی **RemovableStorageDevices** موجود نبود، آن را ایجاد می کنیم.
- درون پوشه ی **RemovableStorageDevices**، یک پوشه به نام **{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}** ایجاد می کنیم.

نکته: مقدار **{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}**، نام **GUID** مربوط به دستگاه های ذخیره سازی **USB** است.

- **value** ای به نام **Deny_Read** و از نوع **DWORD(32 bit)** ایجاد می کنیم.
- وارد تنظیمات این **Value** شده و **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Prevent to write datas on Removable storages

- برای بستن این قابلیت برای یک کاربر خاص، به مسیر زیر می رویم:

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

- برای بستن این قابلیت برای هر کاربری که به این سیستم وارد می شود، به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

- اگر در هریک از مسیرهای بالا، پوشه ی **RemovableStorageDevices** موجود نبود، آن را ایجاد می کنیم.
- درون پوشه ی **RemovableStorageDevices**، یک پوشه به نام **{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}** ایجاد می کنیم.

نکته: مقدار **{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}**، نام **GUID** مربوط به دستگاه های ذخیره سازی **USB** است.

- **value** ای به نام **Deny_Write** و از نوع **DWORD(32 bit)** ایجاد می کنیم.
- وارد تنظیمات این **Value** شده و **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the sharing Tab of folders properties

- به مسیر زیر می رویم:

HKEY_CLASSES_ROOT\Directory\shellex\PropertySheetHandlers\Sharing

- وارد تنظیمات **string value** ی **Default** شده و کافی ست قبل از مقداری که در **Value data** قرار دارد، یک علامت منفی – قرار داده و پنجره را **OK** کنید.

-{f81e9010-6ea4-11ce-a7ff-00aa003ca9f6}

- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Security Tab of drives properties

- به مسیر زیر می رویم:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- وارد تنظیمات value ی **NoSecurityTab** شده و **value data** را از صفر به **یک** تغییر می دهیم.
- اگر این **Value** وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Control Panel from Start menu

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

- **Value** ی **Start_ShowControlPanel** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **Start_ShowControlPanel** دابل کلیک کرده و در تنظیمات آن، **value data** را روی **صفر** قرار می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Disable the Onedrive

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive

- اگر پوشه ی **OneDrive** موجود نبود، آن را ایجاد می کنیم.
- حال یک **Value** از نوع **DWORD(32 bit)** و با نام **DisableFileSyncNGSC** ایجاد می کنیم.
- حال روی **DisableFileSyncNGSC** دابل کلیک کرده و در تنظیمات آن، **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Disable the Windows Store

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore

- **Value** ی **RemoveWindowsStore** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **RemoveWindowsStore** دابل کلیک کرده و در تنظیمات آن، **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Administrative tools from Control Panel

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

- **Value** ی **StartMenuAdminTools** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **RemoveWindowsStore** دابل کلیک کرده و در تنظیمات آن، **value data** را روی **صفر** می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Disable the Task View button

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced

- **Value** ی **ShowTaskViewButton** را پیدا می کنیم.
- وارد تنظیمات آن شده و **value data** را روی **صفر** تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Shutdown button from Start menu

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\Policies\Explorer

- **Value** ی **NoClose** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **RemoveWindowsStore** دابل کلیک کرده و در تنظیمات آن، **value data** را از صفر به **یک** تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Shutdown button from Login screen

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\Policies\ System

- **Value** ی **shutdownwithoutlogon** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **RemoveWindowsStore** دابل کلیک کرده و در تنظیمات آن، **value data** را روی **صفر** تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را **restart** کنیم.

:Disable the Task manager

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

- اگر پوشه ی **System** وجود نداشت، آن را ایجاد می کنیم.
- **Value** ی **DisableTaskMgr** را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال روی **DisableTaskMgr** دابل کلیک کرده و در تنظیمات آن، **value data** را روی **یک** تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:disappearance the Icons in Control Panel

برای اینکه هریک از گزینه های موجود در **Control Panel** را ناپدید کنیم، به شکل زیر عمل می کنیم:

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl

- در این مسیر روی فولدر **DisallowCpl** کلیک راست کرده و از **New** گزینه **String value** را انتخاب کرده و نام آن را **1** تنظیم می کنیم.

- وارد تنظیمات این **value** شده و **Value data** آن را برابر با نام آن گزینه ای که در **Control Panel** قصد پنهان کردن آن را داریم، قرار می دهیم. اما نام گزینه ها یا همان آبجکت های موجود در **Control panel** را باید به شکل کامل وارد کرد، که در زیر، نام کامل برخی، لیست شده اند:

Administrative Tools = Microsoft.AdministrativeTools
AutoPlay = Microsoft.AutoPlay
Biometric Devices = Microsoft.BiometricDevices
BitLocker Drive Encryption = Microsoft.BitLockerDriveEncryption
Color Management = Microsoft.ColorManagement
Credential Manager = Microsoft.CredentialManager
Date and Time = Microsoft.DateAndTime
Default Programs = Microsoft.DefaultPrograms
Device Manager = Microsoft.DeviceManager
Devices and Printers = Microsoft.DevicesAndPrinters
Display = Microsoft.Display
Ease of Access Center = Microsoft.EaseOfAccessCenter
Family Safety = Microsoft.ParentalControls
File History = Microsoft.FileHistory
Folder Options = Microsoft.FolderOptions
Fonts = Microsoft.Fonts
HomeGroup = Microsoft.HomeGroup
Indexing Options = Microsoft.IndexingOptions
Infrared = Microsoft.Infrared
Internet Options = Microsoft.InternetOptions
iSCSI Initiator = Microsoft.iSCSIInitiator
iSNS Server = Microsoft.iSNSServer
Keyboard = Microsoft.Keyboard
Language = Microsoft.Language
Location Settings = Microsoft.LocationSettings
Mouse = Microsoft.Mouse
MPIOConfiguration = Microsoft.MPIOConfiguration
Network and Sharing Center = Microsoft.NetworkAndSharingCenter
Notification Area Icons = Microsoft.NotificationAreaIcons
Pen and Touch = Microsoft.PenAndTouch
Personalization = Microsoft.Personalization
Phone and Modem = Microsoft.PhoneAndModem
Power Options = Microsoft.PowerOptions
Programs and Features = Microsoft.ProgramsAndFeatures
Recovery = Microsoft.Recovery
Region = Microsoft.RegionAndLanguage
RemoteApp and Desktop Connections = Microsoft.RemoteAppAndDesktopConnections
Sound = Microsoft.Sound
Speech Recognition = Microsoft.SpeechRecognition
Storage Spaces = Microsoft.StorageSpaces
Sync Center = Microsoft.SyncCenter
System = Microsoft.System
Tablet PC Settings = Microsoft.TabletPCSettings
Taskbar and Navigation = Microsoft.Taskbar
Troubleshooting = Microsoft.Troubleshooting
TSAppInstall = Microsoft.TSAppInstall
User Accounts = Microsoft.UserAccounts
Windows Anytime Upgrade = Microsoft.WindowsAnytimeUpgrade
Windows Defender = Microsoft.WindowsDefender
Windows Firewall = Microsoft.WindowsFirewall
Windows Mobility Center = Microsoft.MobilityCenter
Windows To Go = Microsoft.PortableWorkspaceCreator
Windows Update = Microsoft.WindowsUpdate
Work Folders = Microsoft.WorkFolders

- برای اینکه یک یا چند آبجکت دیگر از Control Panel را نیز ناپدید کنیم، دوباره باید یک Value از نوع String ایجاد کرده و نام آن را بطورمثال 2 قرار داده و در تنظیمات آن، Value data را برابر با نام آن آبجکت موردنظر قرار می دهیم.

:disappearance the last account in login screen

همانطور که می دانیم، وقتی یک کاربر یک سیستم را روشن می کند و قصد log in دارد، در login screen، جهت ورود به سیستم، نام username آخرین کاربری که در آن سیستم login کرده بوده است را می بینند، پس اگر بخواهیم این آخرین Account حذف شود:

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

- Value ی dontdisplaylastusername را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع (DWORD(32 bit ایجاد می کنیم.
- حال روی dontdisplaylastusername دابل کلیک کرده و در تنظیمات آن، value data را روی یک تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را Restart کنیم.

:disappearance the Snipping tools

- به مسیر زیر می رویم:

KEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TabletPC

- Value ی DisableSnippingTool را پیدا می کنیم.
- اگر وجود نداشت آن را از نوع (DWORD(32 bit ایجاد می کنیم.
- حال روی DisableSnippingTool دابل کلیک کرده و در تنظیمات آن، value data را روی یک تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را Sign Out کرده و دوباره Sign in کنیم.

:Change the User profiles to other directory

بطور معمول، هر User ای که در یک سیستم login می کند، محتویات desktop و یک سری تنظیمات مربوط به آن، در آدرس C:\Users\ ذخیره می شوند.

اما برای اینکه از این به بعد، User profile تمامی User هایی که به این سیستم login می کنند، در یک آدرس دیگر ذخیره شوند، به روش زیر عمل می کنیم:

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

- Value های Default و ProfilesDirectory و Public را پیدا می کنیم.
- وارد تنظیمات هریک از آنها شده و مقدار value data ی آنها را که روی %SystemDrive%\Users تنظیم شده (به معنای همان C:\Users می باشد)، به آدرس جدید موردنظر تغییر می دهیم و OK، مثلاً: E:\Users
- حال این Key (پوشه ی جاری) را (ProfileList) باز می کنیم که با چند Subkey که نام آنها مثلاً با S-1-5 شروع می شود، مواجه می شویم.
- اگر قصد داشته باشیم، User profile حساب جاری را کاملاً به E:\Users انتقال دهیم، ابتدا آن را از جایی که در حال حاضر قرار دارد، به E:\Users کپی می کنیم، و سپس در اینجا، Subkey مربوط به آن را پیدا کرده و وارد تنظیمات Value به نام ProfileImagePath آن شده و مقدار آن را نیز به E:\Users تغییر می دهیم.
- حال فقط کافیست یکبار سیستم را Restart کنیم.
- حال هر کاربر جدیدی که به این سیستم login کند، پروفایل آن در مسیر جدید ساخته و ذخیره خواهد شد.

نکته: بطور مثال در شبکه ها، لازم است که User profile کاربرها را در یک فضای Share شده ی تحت شبکه، ذخیره کنیم، که می توانیم این تغییر آدرس User profile ها را در مکانی روی Server تنظیم کنیم.

:Add Seconds to the taskbar clock

- به مسیر زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

- اگر **Value** ای به نام **ShowSecondsInSystemClock** وجود نداشت، آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- حال وارد تنظیمات **ShowSecondsInSystemClock** شده و در تنظیمات آن، **value data** را روی یک تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

:Enable the automatic registry backup

درحقیقت **Microsoft** تأیید کرده است که عدم پشتیبان گیری خودکار از **Registry**، اقدامی عمدی بوده است، تا بتواند از ظرفیت کلی درایوهای ویندوز کاهش دهد، و پیشنهاد می دهد که از **Restore point** ها استفاده کنیم.

نحوه ی فعال سازی این قابلیت خودکار به شرح زیر است، و مکان **Backup** های خودکار در C:\Windows\System32\config\RegBack می باشد.

- به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Configuration Manager

- **Value** ی **EnablePeriodicBackup** را پیدا می کنیم و اگر وجود نداشت، آن را از نوع **DWORD(32 bit)** ایجاد می کنیم.
- وارد تنظیمات **EnablePeriodicBackup** می شویم.
- مقدار **value data** را روی یک تنظیم می کنیم.
- حال فقط کافیست یکبار سیستم را **Sign Out** کرده و دوباره **Sign in** کنیم.

HOSTS file :

درحقیقت، محل ذخیره سازی تنظیمات جزیی مربوط به هم **DNS Server** و هم **DHCP Server**، یک فایل متنی است به نام hosts ، که در مسیر زیر قرار دارد:

In Windows:

C:\Windows\System32\drivers\etc

In Linux:

/etc/hosts

وقتی که در **address bar** مرورگر، یک آدرس وارد می کنیم (مثلاً www.yahoo.com) این آدرس تبدیل به **IP** شده و برای فراخوانی آن **IP**، **در اولین گام** به فایل hosts مراجعه و آن را بررسی می کند، تا ببینند که آیا اطلاعاتی از این **Page** و **IP** در فایل **hosts** موجود هست یا نه؟ اگر در مورد آن، اطلاعاتی در hosts موجود نباشد، کامپیوتر به سراغ **DNS Server** می رود.

فایل **hosts** در تمام سیستم عامل هایی که از پروتکل **TCP/IP** برای ارتباطات خود استفاده می کنند، به صورت پیش فرض وجود دارد.

توسط حذف یا اضافه کردن برخی محتویات در فایل hosts، می توان ترفندهایی را به کار بست.
بطورمثال اگر بخواهیم یک **Website** را روی **IP** دیگری غیر از **IP** اصلی آن مشاهده کنیم، با اعمال تغییرات در فایل hosts قادر به انجام این کار خواهیم بود.

اما بطور پیشفرض:

- تنها حساب **Administrator** قادر به دسترسی یا باز کردن این فایل می باشد؛
- این فایل بصورت **Read-Only** می باشد.

پس:

- وارد **Properties** شده و در پایین تب **General**، تیک **Read-only** را بر می داریم.
- به تب **Security** رفته و برای **User** موردنظر، **Full Control** را فعال می کنیم.

- لازم به ذکر است که هر خطی که با علامت **#** شروع شود، مورد بررسی توسط سیستم عامل قرار نخواهد گرفت، پس می توان از علامت **#** برای اضافه کردن توضیحات استفاده کرد.

- با توجه به اینکه این فایل، خیلی نقش مهم در دسترسی ها و هدایت های اینترنتی یا شبکه ای کاربر دارد، خیلی از بدافزارها و هکرها، به دنبال آن خواهند بود. پس پیشنهاد می شود که:
  - ✓ این فایل را در حالت **Read-Only** و با کمترین **permission** ها، به حساب های غیر **admin** قرار دهیم.
  - ✓ درحقیقت در گذشته، این قابلیت وجود داشت که فایل hosts را با تغییر آدرس پیشفرض آن در **Registry**، جابجا کرد، اما امروزه این قابلیت غیرفعال شده است، درنتیجه، اگر فایل **hosts** را حذف کنیم، سیستم بدون توجه به آن و بدون ایجاد یک نسخه از آن، مسیریابی را توسط **DNS Server** ها انجام می دهد.

- با هر بار **Boot** شدن کامپیوتر، فایل hosts به صورت کامل در **RAM** کامپیوتر قرار خواهد گرفت.
- فایل hosts حجیم، می تواند منجر به کند شدن کامپیوتر شود.

⮚ Block a website :

یکی از ساده ترین و سر راست ترین راه ها جهت بلاک کردن یک وبسایت این است که فایل hosts را باز کرده:

- **به زیر آخرین خط آن رفته و یک سطر جدید را با فشردن Enter، ایجاد کنیم،**
- **آدرس loopback را درج کرده (یعنی 127.0.0.1)،**
- **یکبار دکمه ی Tab را فشرده و سپس آدرس وبسایت موردنظر را درج کنیم.**

و این کار را برای حالت های دیگر آدرس آن وبسایت انجام می دهیم، که از Block کردن آن مطمین باشیم.

مثلاً برای block کردن weblog ای به آدرس: www.pypayam.blogfa.com

```
127.0.0.1        pypayam.blogfa.com
127.0.0.1        www.pypayam.blogfa.com
127.0.0.1        https://pypayam.blogfa.com
127.0.0.1        http://pypayam.blogfa.com
```

- **سپس فایل hosts را save و close می کنیم.**
- **اگر Browser ای باز است، فعلاً آن را می بندیم.**
- **cmd را باز کرده و یکبار حافظه ی DNS cache را توسط دستور زیر تخلیه می کنیم:**

```
ipconfig /flushdns
```

و تمام.

توضیح:

درحقیقت، **ستون اول**، آدرس مقصد است، و **ستون دوم**، آدرسی است که مورد درخواست واقع شده است.

پس وقتی که ابتدا آدرس 127.0.0.1 را و روبرویش آدرس www.pypayam.blogfa.com را وارد می کنیم، منظور این خواهد بود که:

اگر به دنبال www.pypayam.blogfa.com هستی، به آدرس 127.0.0.1 برو، که البته این یک آدرس loopback یا خودی است!

اگر بخواهیم وبسایتی را که از این روش block کردیم، unblock کنیم:

- **در فایل hosts، خطوطی که درج کردیم را delete کرده و فایل را دوباره save می کنیم.**
- **در cmd دستور زیر را وارد می کنیم:**

```
ipconfig /flushdns
```

- **حافظه ی cache مربوط به Browser را delete می کنیم.**

  انجام این کار برای هر مرورگری، به شکل خاص خودش انجام می شود.

⮚ Reset the hosts :

برای بازگرداندن فایل **hosts** به حالت اولیه، کافی ست یک فایل **notepad** باز کرده و متن زیر را درون آن وارد کرده و فایل را با نام **"hosts"** ذخیره کنیم:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
```

حال به آدرس C:\Windows\System32\drivers\etc رفته و فایل hosts حاضر را به چیزی دیگر تغییرنام می دهیم.

سپس فایل hosts جدید را در آنجا **paste** می کنیم.

اگر همه چیز برقرار و مرتب بود، می توانیم فایل hosts قدیمی را حذف کنیم.

Bitlocker :

Bitlocker، روش رمزنگاری کردن کامل یک Drive است.
عملکرد این رمزنگاری طوری است که اگر کسی Hard drive را از سیستم جدا کرده و آن را در یک سیستم دیگر متصل و سعی در فراخوانی محتویات آن داشته باشد، فوری با صفحه ی درخواست Bitlocker Key مواجه می شود که بدون گذر از این صفحه، هیچ کاری جهت دسترسی به محتویات آن درایو، از دستش بر نمی آید، مگر اینکه Hard drive را بطورکامل format یا wipe کنیم.

Bitlocker آنقدر خودکار عمل می کند، که در مورد آن می توان گفت: Set it and forget it.

پیشنیاز یک فعالسازی سهل و کامل Bitlocker، وجود قطعه ی سخت افزاری TPM chip بر روی mainboard است.
البته که بدون TPM Chip هم می توان آن را فعال کرد، اما:
- ✓ یا باید هربار که سیستم را روشن می کنیم، Bitlocker key را بصورت دستی وارد کنیم.
- ✓ و یا Bitlocker key که طی فرآیند فعال سازی Bitlocker تولید شده بوده است را روی یک USB flash ذخیره می کنیم، و آن را به سیستم متصل می کنیم.

- برای بررسی Bitlocker، می توان PowerShell را با دسترسی Admin باز کرده و دستور زیر را وارد کرد:

```
Get-Tpm
```

اگر دستگاه دارای TPM Chip باشد، مقدار TpmPresent باید True باشد.

- یک روش گرافیکی جهت اطمینان از وجود TPM chip بر روی سیستم، این است که وارد کنسول TPM شویم: در RUN: tpm.msc
- باید در قسمت Status عبارت The TPM is ready for use قابل مشاهده باشد.

- در صورتی که آیکون درایو، به شکل  تغییر کرده باشد، به معنی فعال بودن Bitlocker است.
- در صورتی که دیسک را کاملاً format کنیم (محتویات آن نیز حذف می شوند)، Bitlocker key نیز حذف شده و می توان از دیسک، استفاده ی مجدد کرد.

نکته: درحقیقت فایل سیستم EFS در ویندوز، خودش مانند یک Bitlocker عمل می کند؛ با این تفاوت که بجای اینکه تمام دیسک را یکجا رمزنگاری کند، تنها فایل ها یا directory هایی که برای آن تعیین می کنیم را رمزنگاری می کند، به همین جهت، سرعت رمزنگاری EFS نیز سریعتر از Bitlocker می باشد.

نکته: درصورت نیاز به به روز رسانی Firmware های سخت افزاری یا به روزرسانی های سیستم عامل، اگر، Bitlocker همچنان فعال باشد، در restart بعدی سیستم، نیاز به وارد کردن Bitlocker Key خواهیم داشت.
راه حل، این است که قبل از اجرای به روزرسانی ها، Bitlocker را به حالت Suspent یا تعلیق در بیاوریم، و در پایان به روزرسانی، دوباره آن را فعال یا Resume کنیم.

Tips:

- تمامی لوازم الکترونیکی و کامپیوتری، با برق DC کار می کنند و نه AC، چون برای لوازم الکترونیکی، نوسانات برق، قابل پذیرش نبوده و سیستم فوراً خاموش خواهد شد. به همین جهت بطورمعمول همه ی آنها دارای یک آداپتور تبدیل AC به DC هستند.
- هر شبکه ای که نیاز به اتصال به شبکه ی ISP داشته باشد، یک WAN است.
- هرآنچه که در Windows Services یا کنسول Services اجرا می شود، برای تمام Account های کاربران کامپیوتر اجرا می شود، یعنی مختص به دستگاه کامپیوتر است، نه User Account.
- برای باز کردن یک فایل، توسط یک حساب (Account) دیگر، ابتدا از روی Keyboard دکمه ی Shift را نگه داشته و بعد کلیک راست کرده و Run as a different User را می زنیم.
- برای باز کردن کنسول Task manager و یا کنسول mmc با دسترسی Admin، cmd را بصورت Run as Administrator باز کرده و وارد می کنیم : taskmgr و یا mmc
- به دکمه های Fn روی کیبورد، Toggle Function key هم گفته می شود.
- به درگاه کابل برق روی لپتاپ، DC Jack گفته می شود.
- به هر نرم افزاری که مثل یک بانک داده برای مدیریت و کنترل اموال، منابع و دارایی های شرکت بکار گرفته می شود، ERP یا Enterprise Resource Planning گفته می شود.
- ورود به سیستم به شکل Multi-Factor Authentication یا MFA یعنی علاوه بر اطلاعات Credential مربوط به User، یک یا چند روش ورود دیگر نیز (Two-Factor Authentication) جهت ورود به سیستم، پیش نیاز باشد. مثل اثرانگشت، تشخیص چهره، اسکن چشم، کارت و ...
- ورود به سیستم توسط شناسایی اعضای بدن یا رفتارهای فیزیکی شخص، مثل اثرانگشت و ... را Biometric Authentication می گویند.
- ماده ی مصرفی پرینتر سه بُعدی را Filament می گویند.
- در DHCP Server آدرس چاپگرها و دستگاه های مشابه را reserve می کنیم.
- وقتی یک لبتاپ برای شارژ و روشن ماندن، نیاز به وصل کردن شارژر به برق دارد و درغیراینصورت خاموش می شود، باید باطری لبتاپ را عوض کرد.
- اگر یک پروژکتور بعد از مدتی روشن بودن، صفحه اش خالی شد و تصویر ارسال نکرد، مشکل از Fan خنک کننده اش است که باید تعویض شود.
- اینکه کارت Graphic سیستم، خیلی قوی باشد، مهم نیست، اگر توان PSU قادر به پشتیبانی آن نباشد، سیستم خاموش خواهد شد.
- بطور معمول، کابل ها به شکل حلقوی به دور خود پیچیده شده و بسته بندی می شوند.

  فرض کنید یک کابل بسته بندی شده داریم که از اندازه ی آن را نداریم.

  از آنجا که شکل پیچش و بسته بندی، دایره وار است، سریع ترین روش اندازه گیری طول کابل، این است که محیط یک پیچش دایره ای را حساب کرده و در تعداد حلقه ها یا پیچش های کابل ضرب کرد. (با فرض 3 برای عدد π)

  محیط دایره:

$$P=\pi.d \text{ (قطر دایره)}$$

- هیچگاه دسترسی Full Control را به کاربران دیگر نمی دهیم، و فقط برای Owner آن فایل، فعال خواهد بود.
- در DNS Server تنها آدرس های Site ها و آدرس های Client های موجود در شبکه، ذخیره می شوند.

  در Branch Cache Server، همراه با آدرس های Website ها، محتویات آنها نیز ذخیره می شوند.

  وظیفه ی این Server این است که فایل هایی که در Remote قرار دارند و کاربران آنها را درخواست داده بودند را در خودش ذخیره کند، تا در آینده، در صورت بی تغییر ماندنِ آنها در Remote Server، آنها را از سمت خودش ارائه دهد.

- فرض کنید با یک **User account** معمولی به شبکه **login** کرده اید، اما نیاز دارید که یک کنسول را با دسترسی مدیریتی فراخوانی کنید. پس **Cmd** را به صورت **run as administrator** باز کرده و برای هریک از کنسول هایی که در زیر آمده است، دستور یا عبارت مربوط به آن را درج و وارد می کنیم:

Cosole name	Command
Task manager	taskmgr
Device manager	devmgmt.msc
MMC	mmc
Disk management	diskmgmt.msc
Windows Registry	regedit

Security :

درحقیقت، امنیت، شامل سه بخش کلی می باشد:

- ✓ امنیت در برابر حملات خارجی، که عمدی و ساختگی می باشند، که ویروس ها و بدافزارها هم شامل این دسته هستند.
- ✓ امنیت در برابر حوادث ناخواسته، مثل قطعی برق، نوسانات برق، از کار افتادن دستگاه ها، حوادث طبیعی، انفجارها و ... .
- ✓ امنیت فیزیکی در محیط شبکه.

حملات (Attacks):

- ➢ **Spoofing**: وقتی هرکسی یا هرچیزی، به هرشکلی با شما تماس می گیرد و خودش را به عنوان کسی یا چیزی که شما می شناسید، معرفی می کند، نوعی حمله ی **Spoofing** صورت گرفته است.
  - یکی از این نوع حملات در شبکه های بزرگ، **man in the middle** (**MiTM**) می باشد.
  - یکی از معمول ترین **Spoofing** ها، **Email Spoofing** می باشد که یک ایمیل مشابه با یک سایت کاملاً آشنا برای شما (مثلاً مشابه **Gmail.com**) ارسال می شود، در حالی که اگر به آدرس فرستنده ی آن دقت کنید، می بینید که یک آدرس غیرمتعارف و متفاوت از سایت **Gmail** است. و حال کافی ست که روی محتویات آن ایمیل کلیک کنید تا حمله کننده (**Attacker**) به یک شکلی شما را به دام بیندازد!

- ➢ **Phishing** : هرگونه تلاشی، جهت بدست آوردن مشخصات شخصی شما مثل **username** و **password** و ... از هر طریقی (مثلاً توسط یک صفحه ی جعلی، و یا فریب دادن شما و یا حتی دریافت آن اطلاعات به صورت مستقیم و بی دردسر) **Phishing** نامیده می شود.

- ➢ نوع مشابه، اما پیشرفته تر و خطرناک تری از **Phishing** وجود دارد، به نام **whaling**، که درخواست اطلاعات یا درخواست تایید های حساس تری مثل تراکنش های مالی، به افراد سطح بالاتر سازمان ها مثل رئیس و مدیرعامل ارسال می شوند.

- ➢ نوعی حمله وجود دارد به نام **Dumpster Diving** که بر طبق آن، مهاجم سطل زباله ی مقصد را جستجو می کند تا فایل های سازمانی مفید پیدا کند!
  به همین جهت، بهترین کار این است که فایلهای حساس شخصی یا سازمانی را بطورکل و مستقیم نابود کنیم. (**destruct**)

- ➢ وقتی هکرها به یک بخش آسیب پذیر که هنوز مسئول های شبکه متوجه آن نشده اند و به آن رسیدگی نشده است، حمله می کنند، به این حمله **Zero-Day attack** گفته می شود.

برخورد با Ransomware و Malware (بد و باج افزار) ها و Virus (ویروس) ها:

وقتی یک کاربر عضو شبکه اعلام می کند که سیستم دچار ویروس یا بدافزار شده است، به شکل زیر عمل می کنیم:

- **Symptoms** (علایم) آن ویروس یا بدافزار را شناسایی می کنیم.
- ارتباط سیستم را با هرگونه شبکه، بطورکامل قطع می کنیم. (Quarantine the PC)
- توسط **Antimalware** یا **Antivirus**، سیستم را پاکسازی و نشانه های آن را رفع می کنیم.
- در بخش **Updates**، آخرین **windows update** ها را دریافت می کنیم.
- **Antivirus** را برای **Scan** های هفتگی زمانبندی می کنیم.
- کاربر را آموزش می دهیم که از این به بعد به چه شکل رفتار کند که راه را برای بدافزارها باز نکند.

Backup:

توصیه های پیش و پس از راه اندازی فرآیند Backup:

- **برای Server Backup، نسخه ی Backup را در خارج از Server، ذخیره و نگهداری می کنیم.**
- **نسخه ی Backup را روی Hard Disk ذخیره نمی کنیم؛ بلکه بر روی Tape.**
- **فرآیند Backup را به شکل زمانبندی شده انجام می دهیم، طوری که شامل دو بازه ی زمانی کوتاه و بلند مدت باشد؛ بطورمثال:**
  - ساعت 12 نیمه شب، هر روز
  - ساعت 12 نیمه شب، هر یکشنبه ی آخر ماه
- **نسخه های Backup را هر چند وقت یکبار تست می کنیم.**
- **اگر بخواهیم از صحت ایجاد فایل های Backup اطمینان پیدا کنیم، بهترین کار این است:**
  - برای Error های هریک از Backup ها، alert تعریف کنیم.
  - برای اتمام کامل فرآیند Backup، اعلان (Notification) تعریف کنیم.

Cloud / Off-Premise / On-Premise:

به هر لوازمی که در محیط اداره یا سازمان، راه اندازی شده باشد، On-Premise **گفته می شود، و اگر خارج از محیط، راه اندازی شده باشند،** Off-Premise **گفته می شود.**

- ✓ **از مزایای On-Premise Backup این است که در صورت نیاز به Recovery، سرعت بالایی خواهد داشت.**

گاهی در نتیجه ی یک حادثه، مثل سیل، زلزله و تخریب، انفجار و ... ، Server یا Server های موجود در اداره، طوری تخریب می شوند، که هم فایل ها و هم Backup ها از دست می روند. به این وضعیت، Disaster یا فاجعه گفته می شود.

- ✓ **پس عواقب Disaster، از معایب On-Premise Backup می باشد.**

راه حلی وجود دارد به نام Hot Site، که نوعی Disaster Recovery Plan است و برطبق آن، در یک مکان دیگر از محل اداره (شبکه)**، تمامی تجهیزاتِ لازم جهت replication** (به روزرسانی فوری) **با شبکه ی اصلی برقرار بوده و نوعی Backup امن در صورت وقوع Disaster می باشد، و در صورت قطع شدن کامل شبکه ی اصلی، این Hot Site، همچنان شبکه را برقرار نگه می دارد.**

اما راه حل مدرن تری که جهت متمرکزسازی (centralize کردن) **Backup های یک سازمان استفاده می شود، Cloud replication می باشد.**

:Hardware security

- بهترین روش های افزایش امنیت اتاق **Server**:
  - راه اندازی قفل درب یا **Door lock** توسط یکی از دو روش زیر:
    - استفاده از دستگاه علامتخوان یا کارت خوان (Badge reader)
    - استفاده از قفل بیولوژیکی (biometric lock)
  - راه اندازی پنجره ی امنیتی یا **Privacy window**

فرض کنید بخواهیم یک دستگاه مثل **Server** و یا یک **Computer** یا **Laptop** را باز کنیم:

- اولین اقدام، قطع کردن برق **power** می باشد.
- سپس دستبند **ESD Strap** (electrostatic-sensitive device) را به دست می کنیم:

این دستبند، جهت محافظت از شوک الکتریکی و برق گرفتگی کامل، که ناشی از اتصال کوتاهی که میان دستگاه های برقی و بدن انسان خواهد بود، به دست بسته می شود.



- جهت امنیت بیشتر، از **ESD mat** که یک صفحه ی عایق می باشد نیز استفاده می کنیم.



- وقتی بخواهیم قطعات سخت افزاریِ کارت شکل را با دست بگیریم، بهتر است که از لبه ها، آنها را بگیریم که از لمس شدن سطحِ مداریِ آنها توسط دستهایمان، جلوگیری شود.

:Tips

- زمانی که از اینترنت شخصی استفاده می کنیم، (که هیچ Web Server ای و یا هیچ Web server غریبه ای، میان دستگاه شما و محیط اینترنت وجود ندارد) در تنظیمات Firewall ویندوز، تنها **private network** را فعال می کنیم؛ که در این صورت، دستگاه به شکل discoverable یا قابل دیده شدن در شبکه حضور خواهد داشت و اعضای حاضر در شبکه، آن را خواهند دید.
- زمانی که از اینترنت دانشگاه یا ... استفاده می کنیم، (که Web Server شبکه ی دانشگاه یا ... میان دستگاه شما و اینترنت قرار دارد) در تنظیمات Firewall ویندوز، تنها public network را فعال می کنیم، که در این صورت دیگر discoverable نخواهد بود.
- منظور از اینکه گفته می شود یک سیستم عامل را harden کنیم، (system hardening) این است که آن سیستم را مجهز به به روزترین update ها و Security Settings کنیم، طوری که در امن ترین حالت ممکن قرار بگیرد.
- کامپیوترهایی که نرم افزارهای outdated دارند، بیشترین آسیب پذیری را در برابر حملات بدافزارها دارند.
- در صورتی که یک کاربر شخصی نیاز به یک Antivirus داشته باشد که هزینه بر هم نباشد، می توان نوع open license یا همان open source را به او پیشنهاد کرد.
- وقتی می گوییم برای یک Port روی Switch یا Router، وضعیت Port Security را فعال کرده ایم، یعنی یکی از موارد زیر:
  - وقتی دستگاهی بخواهد توسط آن Port به شبکه وصل شود، mac address آن بررسی می شود که جزو آدرس های مجاز است یا خیر.
  - Certificate Security برای آن Port فعال شده است، پس دستگاه موردنظر باید دارای Certificate مجاز برای اتصال باشد.
- جهت حفظ امنیت دستگاه های سیار در برابر تهدیدات و حملات، یک مجموعه سیاست امنیتی وجود دارد، به نام MDM یا Mobile Device Management.
- سیاستِ PoLP یا همان principle of least privileges یا «اصل کمینه سازی حق ویژه»، به این اشاره دارد که هر کاربر تنها به آن بخش از اطلاعاتی که برای وظیفه اش نیاز دارد، مجوز داشته باشد.
- فرض کنید جهت login به لب تاپ، هم توسط Username و Password و هم با وارد کردن اثرانگشت بتوانیم اقدام کنیم، به این سیستم امنیتی، multi factor گفته می شود، در صورتی که اگر تنها توسط User و Password ممکن می بود، به آن Single factor گفته می شد.
- می دانیم که وقتی یک دستگاه خارجی، مثل دستگاه هایی که رابط USB دارند را به کامپیوتر متصل می کنیم، یک Autorun menu یا Autoplay menu ظاهر می شود، که این menu می تواند راه را برای جابجا و منتقل شدن مستقیم بدافزارها به درون سیستم هموار کند. پس جهت حفظ بیشتر امنیت سیستم های عضو شبکه، این قابلیت را خاموش می کنیم، که باید وارد AutoPlay Settings شویم.
- یکی دیگر از راه های حفظ امنیت سیستم های متصل به شبکه، غیرفعال کردن حساب Guest در آنهاست.
- هرگاه یک کاربر با User account اش در حال انجام کارهای عجیب است، ابتدا فوری حساب او را disable می کنیم.
- فرض کنید، روی Laptop سازمانی شما، یک یا تعدادی map drive مربوط به شبکه ی سازمان وجود دارد. حال فرض کنید، از سازمان خارج شوید، در یک هتل، به اینترنت هتل متصل شده و بخواهید به فایل های سازمانی تان دسترسی داشته باشید، پس VPN مربوط به شرکت را روی Laptop روشن می کنید، و سپس map drive ها دوباره متصل شده و به همه ی محتویات دسترسی خواهید داشت. اما نکته اینجاست که هرکسی که به شبکه ی هتل متصل باشد نیز، قادر به دسترسی به map drive های سازمانی شما که روی سیستم شما mounted شده اند، خواهد بود! بهترین کار، بستن یا unount کردن MAP drive ها در هنگام اتصال به شبکه ی غریبه است.
- بطورمعمول برای کنترلِ ورود و خروج پرسنل به ساختمان شرکت، و یا حتی جهت استفاده از برخی دستگاه های سازمان، مثل Printer ها، از یک قطعه ی الکترونیکی/بلوتوثی کوچک استفاده می شود به نام Key fob که بصورت Remote control قابل تنظیم است؛ مشابه دزدگیر خودرو.
- وقتی یکی از پرسنل شرکت، یک ایمیل مزاحم دریافت می کند، جهت جلوگیری از ارسال های بیشتر آن، باید فیلتری بر پایه ی آدرس mail Server آن ایمیل مزاحم ایجاد کنیم. پس مدیر شبکه باید آدرس mail Server آن ایمیل را پیدا کرده و آن را در Spam مربوط به mail Server شبکه قرار دهد. که به این کار Domain-based Filter گفته می شود.
- Server باید همیشه با latest security updates به روز باشد تا از هرگونه آلودگی یا نفوذ، در امان باشد.

Laptop / Smartphone / Tablet :

- به این قابلیت که روی **Laptop**، درگاه سیم کارت وجود داشته و قادر به دریافت امواج تلفن و اینترنت می باشد، **cellular** گفته می شود.
- برای صرفه جویی در مصرف باطری، **Bluetooth** و **Cellular** را خاموش می کنیم.
- پرداخت غیرتماسی، توسط کارت های بانکی، توسط فناوری **NFC** انجام می شود. که لازمه ی آن، فاصله ی کمتر از **4** سانتی متر است.
- در **Leptop** ها، به بخش مخصوص جایگیری **LCD** گفته می شود: **Bezel** که هنگام تعویض **LCD** اولین بخشی ست که امکان صدمه دیدنش وجود دارد.
- وقتی **LCD** یک لپتاپ را تعویض می کنیم، باید بررسی کنیم که آنتن دهی **WiFi** آن تغییر نکرده باشد!
- اگر روی یک **Laptop** آب ریخته شود، چای پیچ ها رو علامت زده و سپس آنها را باز کرده و درب لبتاپ را باز می کنیم. قطعات را جدا کرده و صبر می کنیم که همگی خشک شوند.

- بطور معمول **Touch Screen** مربوط به دستگاه های موبایل یا تبلت، از نوع خازنی یا **Capacitive** هستند.
- در حالت **Airplane mode** نه می توان به کسی زنگ زد و نه کسی می تواند به ما زنگ بزند و نه می توان از **WiFi** استفاده کرد.
- به **App** هایی که در دستگاه های **mobile**، جهت دسترسی و مدیریت **Email** های مان نصب می کنیم، نرم افزار ایمیل شخص ثالث یا **third-party email software** گفته می شود.
- برای حفظ امنیت دستگاه های **mobile** مثل تلفن های سیار، در صورت دزیده یا مفقود شدن، **feature** مخصوص **remote wipe** را روی آنها نصب کرده و تمام سیستم دستگاه را **encrypt** می کنیم.
- به جهت استفاده ی صحیح و به جا و متعارف از امکانات الکترونیکی موجود در یک شرکت، قاعده ای وجود دارد که همه ی پرسنل باید با آن موافقت کنند، به نام **AUP** (acceptable use policy)؛ که بهترین روش جهت کاهش دردسرها و مسئولیت ها در برابر مشکلات امنیتی می باشد.
- وقتی **Stylus** (قلم نوری) مربوط به **Tablet**، روی صفحه ی آن، تشخیص داده نمی شود و کار نمی کند، می توان یکبار ارتباط آن را قطع و از نو وصل کرد تا دوباره متصل و شناخته شود.

Troubleshoting:

Low Speed PC:

- ابتدا از **TaskManager** قدرت **RAM** و **CPU** و مابقی قطعات را بررسی می کنیم.
- سپس میزان فضای ذخیره سازی موجود را بررسی می کنیم.
- و بعد قدرت **NIC** و سرعت آن را بررسی می کنیم.
- بعد اگر **Antivirus** موجود باشد آن را قطع و وصل می کنیم.

Driver error or Hadware improvement:

- اگر خطایی مربوط به درایورها یا مربوط به **Registry** ویندوز نمایش داده می شود؛
- و یا فکر می کنید که سیستم دچار ضعف یا آلودگی نرم افزاری شده است،
- و یا اینکه ظاهراً **Storage** دچار مشکل شده است و نیاز به ترمیم و چک و بررسی سلامت دارد،

می توان توسط ابزار **dism** روی آن کار کرد.

پس **Command Prompt** را به صورت **Run as administartor** اجرا کرده و دستورهای زیر را یکی یکی وارد می کنیم:

```
Dism /Online /Cleanup-Image /CheckHealth
Dism /Online /Cleanup-Image /ScanHealth
Dism /Online /Cleanup-Image /RestoreHealth
```

Resolve network issues:

برای رفع مشکلات شبکه در یک سیستم، و یا در مواجهه با **error** هایی شبیه به *Windows update can not currently check for updates* و یا زمانی که اتصال به اینترنت یا شبکه عجیب به نظر می رسد، طوری که ارتباط وجود دارد، اما آیکون کوچک در **task bar** (**System tray**) نشان از قطعی ارتباط دارد:

ابتدا **DNS** را **restart** می کنیم؛ پس با دسترسی **admin**، وارد **cmd** شده و دستورات زیر را یکی یکی وارد می کنیم:

```
Ipconfig /flushdns
Ipconfig /release
Ipconfig /renew
```

اگر مشکل همچنان برطرف نشده باشد، سرویس های **Network** را **restart** کنیم؛ پس با دسترسی **admin**، وارد **cmd** می شویم و دستورات زیر را یکی یکی وارد کرده و درپایان کامپیوتر را یکبار **restart** کرده و دوباره چک می کنیم:

```
netsh int ip reset reset.txt
netsh winsock reset
netsh advfirewall reset
```

اگر پس از **restart** کردن سرویس های **Network** و سپس خود سیستم، همچنان مشکل برطرف نشده باشد؛
ارتباط با شبکه را بطورکامل قطع می کنیم؛ همزمان **modem** یا **router** شبکه را نیز بطورکامل خاموش می کنیم.
پس از چند ثانیه، دوباره **modem** را روشن کرده و ارتباط کامپیوتر با آن را برقرار کرده و روشن کرده و دوباره تست می کنیم.

No Internet

گاهی وقت ها، اتصال فیزیکی با اینترنت برقرار است، اما هیچ سایت و نرم افزاری متصل نمی شود.

مثلاً در مرورگرها، پیغام name not resolved **مدام ظاهر می شود.**

و در cmd هم به هیچ سایتی هم Ping نمی شود، به جز یک سری Forwarder معروف، مثل 8.8.8.8 یا 4.2.2.4!

در اینجا باید به صورت دستی، برای DNS Server خود سیستم، آدرس یک یا دو عدد از همین Forwarder ها را درج کرد.

:System turned On but doesn't come up

- **تمام Flash memory ها را جدا کرده و دوباره تست می کنیم.**
- **در تنظیمات BIOS، باید دستگاه ذخیره سازی را شناسایی کرده باشد.**
- **در تنظیمات Boot BIOS باید دستگاه ذخیره سازی بر روی حالت default باشد.**
- **اگر بطورکامل چیزی به نمایش در نمی آید، مشکل از Bios Update است که باید upgrade یا Downgrade شود.**

:System suffers from continuously restart

- **به معنی ایراد Ram سیستم است.**

:System turned On with "No Secure" Error

سیستم روشن می شود، اما مانیتور خطای No Source نشان داده و صدای بوق از کیس می آید.

- **نشانه ی ناکافی بودن Power برای PC است.**

:System turned On with "No OS found" Error

سیستم روشن می شود، اما مانیتور خطای No OS found نشان می دهد.

- **به هردلیلی، در تنظیمات Bios گزینه ی Boot partition جابجا شده است، که در نتیجه، سیستم درخواست پیدا کردن OS را به یک دیسک یا رسانه ی دیگر (مثل DVD Rom یا PXE Boot یا USB flash memory) ارسال می کند.**

:Touch Screen of a Notebook or Tablet works disordered

- **باید ابتدا Driver مربوط به Touch Screen آن را update کرد.**

:Output of a Printer includes garbled Text

- **به دلیل عدم Update درایور پرینتر می باشد.**

:Print-Output of a MAC includes garbled Text

- **باید نسخه ی macOS درایور پرینتر را روی Print Server نصب کنیم.**

:CPU over temperature, Press F1 to Resume

- **مشکل از Bios Update است که باید Upgrade یا downgrade شود.**

BIOS Update

جهت نصب ویندوز روی یک دستگاه، معمولاً Laptop ها، در دو حالت می توانیم و یا اینکه مجبور هستیم، BIOS را به روز رسانی کنیم:

- **دیسک ذخیره سازی، از نوع NVMe باشد.**
- **اعتبار warranty آن باطل شده باشد.**

:A notebook doesn’t boot anymore

1. **Turn off for some Seconds and try again**
2. **Check the power supply and Charger**
   Power supply cable and Adapter for the right voltage
   You can test the output DC-Voltage with a Voltmeter or Multimeter: RED(+) goes inside the hole of Plug
3. **Test with a spare Charger**
4. **Check the Screen**
   Try disconnecting any external displays
   If the laptop appears to be booting fine, but there’s no image at all, the LCD panel could be at fault!
5. **Remove and reinstall components**

:(blue Screen of death) BsoD

اولین اقدام ضروری این است که تمام وسایل جانبی متصل به سیستم را جدا کنیم و دوباره امتحان کنیم. (**USB** و حافظه های جانبی و ...)

دلیل ظاهر شدن این صفحه های آبی، بطور معمول:

- مشکل درایور سخت افزار:
  باید **Driver** یکی از سخت افزارها را (مثلاً **Printer** معمولاً)، به روز کرد.
- مشکلات سازگاری سخت افزاری:
  معمولاً به صورت IRQL_NOT_LESS_OR_EQUAL نشان داده می شود که به معنی ناسازگاری یکی از قطعات با بقیه اجزا می باشد.
- داغ شدن اجزای سخت افزاری:
  می توان با اضافه کردن **FAN** و خنک کردن سیستم این مشکل را حل کرد!
- مشکل در **RAM**:
  معمولاً به صورت BAD_POOL_HEADER نمایش داده می شود، یا اتصال آن شُل شده و یا دارای مشکل جدی تری است.
- مشکل در تنظیمات **BIOS**:
  تنظیمات **BIOS** بسیار حساس هستند و اعمال تغییرات در آنها می تواند باعث بروز این صفحه شود، که باید تنظیمات را **reset** کرد.
- مشکل **Hard Drive**:
  احتمال وجود **Bad Sector** و یا خرابی در قطعات **Hard Disk** وجود دارد و اشکال در اتصال کابل آن به **Main board**
- وجود **Virus**
- افزایش میزان فایل های موقت یا **temp files** در ویندوز در پوشه ی **temp** در درایو **C**: که باید حذف شوند.
- **Update** نبودن ویندوز یا **Driver** ها

: the local print spooler service is not running

سرویس **Print Spooler** کمک می کند تا ویندوز با **Printer** ارتباط برقرار نماید.

گاهی این سرویس از کار می افتد؛ که در نتیجه، درایور **Printer** از کار می افتد و یا در صورت اقدام به نصب درایور، نصب نخواهد شد! پس:

- یا در کنسول **Services.msc** سرویس **Print Spooler** را قطع و وصل می کنیم و یا در **cmd** دو دستور زیر را به ترتیب وارد می کنیم:

net stop spooler
net start spooler

- یا به مسیر **C:\Windows\System32\spool\PRINTERS** رفته و محتویات را پاک می کنیم یا در **cmd** درج می کنیم:

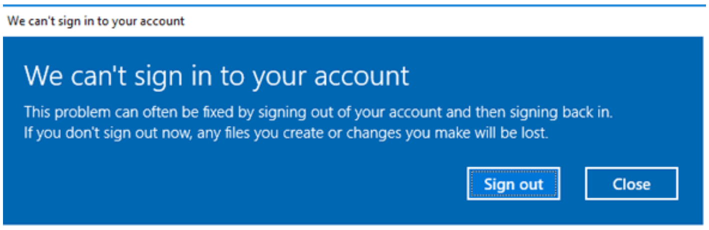
del C:\Windows\System32\spool\printers* /Q

:You've been signed in with a temporary profile / We can't sign in to your account

دو خطا با یک راه حل وجود دارند.

1. خطایی وجود دارد که وقتی به سیستم **login** می کنید، با پیغام زیر در یک کادر آبی رنگ مواجه می شوید:

We can't sign into your account.This problem can often be fixed by signing out of your account and then signing back in. If you don't sign out now, any files you create or changes you make will be lost.



2. پس از **login** به سیستم، خطای زیر به صورت یک **notification** ظاهر می شود:

You've been signed in with a temporary profile.

درحقیقت، احتمال زیادی وجود دارد که **user profile** قدیمی، **load** نشده و سیستم با یک **profile** موقت، اجازه ی **login** داده است.

نکته: **temporary profile** ها نیز مثل **user profile** های ثابت، در اینجا ایجاد می شوند: **C:\Users\TEMP**

پس باید ابتدا **profile** قدیمی را کاملاً حذف کرده و یک **profile** جدید را جایگزین آن کنیم.

- در همان پوشه ی **C:\Users** ،**user profile** قدیمی را یا حذف می کنیم و یا به عنوان راه حل بهتر، تغییر نام می دهیم، به این شکل که در پایان نام آن **.bak** قرار می دهیم و یا در ابتدای نام آن یک **underline** درج می کنیم.
- حال به **Registry** و به مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

- با توجه به اینکه هر **Username** دارای یک **SID** است، در این بین **cmd** را باز کرده و توسط دستور زیر، **SID** حساب موردنظر را می یابیم:

wmic useraccount where name='*username*' get sid

- حال از **subkey** های **ProfileList** هریک را که نام آن با **SID** پیدا کرده در **cmd** مطابقت می کند را حذف می کنیم.

نکته: البته گاهی یکی از آنها پسوند **.bak** را در انتهای نام خود دارد، که اشاره به **Profile** قدیمی دارد، که آن را نیز حذف می کنیم.

- حال کافی ست که یکبار سیستم را **restart** کنیم.

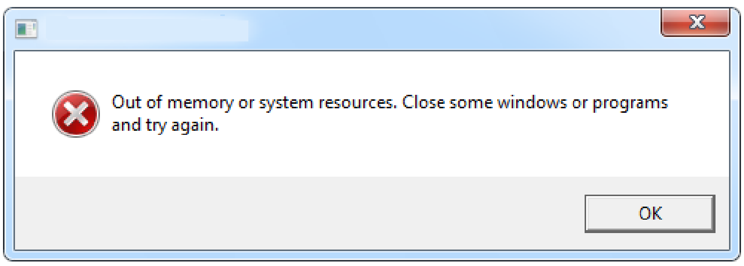
:It takes long to boot to the windows

- اولین ایراد می تواند به حجم فایل های موجود روی **Desktop** اش وارد باشد، که باید آنها را جمع و جور و مرتب و حذف کرد.
- سپس نرم افزارهای **enabled** و غیرضروری در **Startup** را **disable** می کنیم.
- **Hard drive** را **defrag** می کنیم.

:Out of Memory

گاهی به دلیل محدودیت های **desktop** ممکن است پس از باز کردن برنامه و اپلیکیشن های مختلف در **Windows**، نتوانید پنجره ی اضافی دیگری را باز کنید و اگر هم باز شود تمامی اجزا و **Components** های آن به خوبی اجرا نشده و یا به خوبی کار نمی کنند و خطای زیر ظاهر می شود:

Out of memory or system resources. Close some windows or programs and try again.



برای حل این مشکل باید ظرفیت محدود دسکتاپ را تغییر دهیم.

- پس به **Registry** و مسیر زیر می رویم:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ SubSystems

- **Value** ی **Windows** را پیدا کرده و وارد تنظیمات آن می شویم.
- درحقیقت در قسمت **Value data**، مقدار **SharedSection** به صورت مقابل است: SharedSection=xxxx,yyyy,zzzz
- در ویندوز های **32** بیتی باید مقدار **yyyy** را تا **12288** و مقدار **zzzz** را تا **1024** افزایش دهیم.

  در ویندوز های **64** بیتی باید مقدار **yyyy** را تا **20480** و مقدار **zzzz** را تا **1024** افزایش دهیم.

  پس از افزایش این مقادیر به یک مقدار در بازه ی مجاز بالا، پنجره را **ok** می کنیم و تمام.
- حال کافی ست یکبار **sign out** و دوباره **sign in** کنیم.

:Web Password recovery

گاهی در یک وبسایت که دارای یک حساب کاربری هستیم، رمزعبور را فراموش کرده ایم، اما در صفحه ی **login**، به صورت **Cookie** و به شکل نقطه یا ستاره، در نوار **Password** ثبت است، اما دکمه ی **show password** وجود ندارد.

- پس برای مشاهده ی رمزعبور درج شده، کافی ست آن را انتخاب و کلیک راست کرده و **Inspect** را بزنیم.

در کادر باز شده، می بینیم که بخش مربوط به **password** انتخاب شده است، کافی ست در عبارت ”type=”password ، کلمه ی password را با دابل کلیک انتخاب کرده و به جای آن درج کنیم txt و اینتر کنیم.

RAID issue:

file or directory is corrupted and unreadable:

گاهی، یک فایل یا یک پوشه، غیرقابل دسترسی می شود، و پس از تلاش برای باز کردن آن، با خطای زیر مواجه می شویم:

the file or directory is corrupted and unreadable

در این حالت، لازم است که آن درایو را یکبار قطع و بررسی و دوباره وصل کنیم.

این کار را توسط ابزار *chkdsk* (check disk) **انجام می دهیم.**

بطورمثال یک فایل درون درایو D دچار این خطای دسترسی شده است. پس **cmd** **را باز کرده و دستور زیر را وارد می کنیم:**

```
chkdsk /f d:
```

Cloud:

- Cloud Storage، یک فضای ذخیره سازی Online می باشد.
- این Online بودن است که وابستگی فضای ذخیره سازی به جغرافیا و به سخت افزار را از بین می برد.
  (قابل دسترس با هر سخت افزاری و در هرمکانی)
- مثلاً وقتی یکی از پرسنل شرکت، به یک مسافرت کاری بین چند روز تا چند ماه می رود، بهترین گزینه ی دسترسی او به فایل های موردنیازش، ایجاد و اختصاص یک Cloud Storage account به او می باشد.
- به طورمعمول، فضای رایگانی که Cloud های معروف ارایه می دهند، محدود و بین 2 تا 15 گیگابایت است، که افزایش آن، مشمول هزینه می شود.
- همانطور که می دانیم استفاده از Cloud، موجودیت خیلی از سخت افزارها را حذف می کند، در نتیجه، نیازی به گزینه های زیر نخواهیم داشت:
  - کابل کشی (Cabling)
  - خنک کنندگی سخت افزارها و قطعات (Cooling)
  - نصب و نگهداری سخت افزارها و قطعات (Installation and maintenance)

بطورعمومی، سرویس دهی Cloud را به سه دسته تقسیم بندی می کنند:

- **Software as a service (SaaS):** کارآمد برای همه ی کاربران عادی است.
  در این حالت، نرم افزار مورد استفاده ی کاربر، بر روی یک فضای Cloud نصب و راه اندازی شده است، و کاربر جهت استفاده ی آن، کافی ست توسط مشخصات کاربری اش، در هر زمان دلخواه و از هر مکان دلخواه، به آن فضای ابری، Login کرده و نرم افزار را فراخوانی کرده و کارش را انجام داده و نتیجه را ذخیره کند و تمام!
  پس جهت جلوگیری از هدررفتن وقت برای install و update نرم افزاری که کارمندها، فقط هر از گاهی استفاده می کنند، راهکار مناسب، استفاده از SaaS می باشد.
- **Platform as a service (PaaS):** کارآمد برای برنامه نویس ها است.
  مثل یک IDE برنامه نویسی است که در هرزمان و از هرمکان و در هر سیستم عامل، قابل دسترسی است.
- **Infrastructure as a service (IaaS):** کارآمد برای مدیرهای شبکه است که زیرساخت ارتباطی شبکه را کنترل می کنند.

تا به امروز قوی ترین سرویس های Cloud به شرح زیر هستند:

- AWS (Amazon Web Services) از شرکت Amazon : https://aws.amazon.com
- Microsoft Azure از شرکت Microsoft : https://azure.microsoft.com
- Google Cloud از شرکت Google
- Salesforce
- و ...

Regions:

با توجه به اینکه شرکت های Cloud در مناطق مختلفی در سراسر جهان، شعبه دارند، پس از ایجاد یک حساب در یک Cloud و راه اندازی سرویس موردنظر، می توان مشخص کرد که از کدام شعبه یا شاخه ی شرکت، (از لحاظ نزدیکی جغرافیایی، جهت سرعت و دسترسی بهتر) استفاده کند.
برای تعیین این شعبه در AWS به تب Central می رویم.

Azure:

- پورتال یا محیط کار با آژور، ARM (Azure Resource Manager) نام دارد.
- منابع موجود، بر اساس Container ها هستند.
- می توان منابع را گروه بندی کرد و ویژگی هایی را به هریک از گروه ها اختصاص داد.

نکته: در صورتی که یک Cloud environment برای شرکت تدارک دیده باشیم، پرسنل هیچ نیازی به USB flash ها یا DVD و CD ها نخواهند داشت.
تنها کافی ست به سادگی وارد حساب Cloud خود شده و فایل های موردنظر را در آنجا آپلود کرده و یک shared link از آن دریافت کرده و آن Link را به شخص موردنظر ایمیل کنند.

Introduction:

- macOS یک سیستم عامل نسبتاً ساده است که برای کامپیوترهای شرکت Apple طراحی شده است.
- تنها در کامپیوترهای Apple می توان از macOS استفاده کرد.
- mac مخفف macintosh می باشد.
- انواع نسخه های macintosh:
  - mac OS: شامل نسخه های زیر می باشد:
    - Mac OS 1 -9
    - Mac OS x
    - Mac OS x Tiger
    - Mac OS x Leopard
    - Mac OS x snow
  - mac OS mini: شامل نسخه ی Macintosh mac می باشد.
  - mac Server: شامل نسخه ی mac OS x Server می باشد.

- macOS به طور منظم بروزرسانی‌های امنیتی و هر ساله یک بروزرسانی بزرگ دریافت می‌کند.
- macOS بر پایه‌ی سیستم‌عامل «Unix» طراحی شده است که ریشه‌ی آن به دهه‌ی 1970 میلادی بر می‌گردد.
- شباهت‌های زیادی بین macOS و توزیع‌های مختلف سیستم عامل Linux و Unix وجود دارد که به عنوان مثال می‌توان به رابط خط فرمان «Bash» و سطوح مجوزهای Unix اشاره کرد.
- macOS سیستم‌عامل سر راستی است. مجموعه‌ای از نرم‌افزارها که برای کارهای روزانه مورد نیاز هستند، مثل مدیریت ایمیل یا Web browser را از زمان نصب در خود دارد و به خوبی با سایر دستگاه‌های خانواده‌ی Apple مثل IPHONE و IPAD کار می‌کند.
- برای استفاده از مواردی نظیر«iCloud» ، «App Store»، «iTunes»و سایر سرویس‌ها، نیاز به یک Apple ID خواهید داشت.
- اگر از قبل در Iphone یا IPAD خود، یک Apple ID داشته بوده باشید، می توانید از آن برای کامپیوتر mac خود استفاده کنید، در غیر این صورت باید یک Apple ID بسازیم.

- Laptop های شرکت Apple دو دسته هستند:
  MacBook Air و MacBook Pro که نسخه ی Pro پیشرفته تر و با امکانات بیشتر می باشد.

:macOS installation on Vmware

- پس از دانلود یا تهیه ی **Image** سیستم عامل **mac**، فایلی وجود دارد به نام **unlocker for macOS** که آن را نیز باید دانلود کرده و از حالت فشرده خارج کنیم.
- **VM** های موجود در **Vmware** را بطورکامل خاموش کرده و بطورکامل از **Vmware** خارج می شویم.
- وارد پوشه ی **unlocker for macOS** شده و فایل **win-install.cmd** را بصورت **Run as administrator** اجرا می کنیم.
- پس از آن، وارد **Vmware** شده و **Create a new VM** را می زنیم.
  - آن را از نوع **typical** انتخاب می کنیم.
  - گزینه ی **I will install OS later** را می زنیم.
  - **Apple mac** را می زنیم.
  - حجم **Disk** آن را حدود **120 GB** و به صورت **as a single file** درج می کنیم.
  - وارد تنظیمات آن شده و مقدار را بالای **4GB** و مقدار **CPU** را حداقل دو **CPU** با دو **core** درج می کنیم.
  - فایل **ISO** سیستم عامل را توسط **DVD Rom** آن، انتخاب می کنیم.
  - **Finish** کرده و **VM** را روشن می کنیم.
- پس از روشن کردن **VM** و ورود به مراحل نصب، به عنوان اولین **option**، باید زبان را انتخاب کنیم.
- سپس در پنجره ی ظاهر شده ی بعدی، احتمالاً خطا می دهد که فضای دیسک کافی نیست! پس از منوی بالا، **Utilities** و **Disk utilities** را می زنیم.
- گزینه ی **Vmware Virtual SATA Hard Drive Media** را انتخاب کرده و در بالا، روی **Erase** می زنیم.
- در کادر باز شده، برای **Name**، یک نام درج می کنیم، مثلاً: **macOS HD** و برای **Format** درج می کنیم: **(..mac OS X Extended (J** و برای **Scheme** درج می کنیم: **GUID Partition MAP** و سپس روی **Erase** کلیک می کنیم.
- پس از پایان **Disk erase**، روی **Done** زده و از منوی بالا، روی **Disk Utility** کلیک کرده و **Quick Disk Utility** را می زنیم.
- دیسکی که ایجاد کردیم را انتخاب کرده و **Continue** را می زنیم.
- پس از اتمام راه‌اندازی اولیه ی مک، سیستم **Restart** خواهد شد. پس از بالا آمدن، یک **Desktop** خالی به همراه تعدادی آیکون در پایین صفحه (که به آن داک می‌گویند) مشاهده می‌کنید.

Mac Environment:

محیط کلی mac شامل سه قسمت است:

❖ Manu bar در بالا: این نوار بر اساس پنجره یا نرم افزاری که باز باشد، تغییر می کند، اما در Desktop شامل سه بخش است:

- **Apple menu** (آیکون Apple):
  - **App Store**: نرم افزارهای مربوط به سیستم عامل mac را می توان بطور مستقیم در این بخش پیدا و نصب کرد.
  - **Force Quit**: وقتی یک نرم افزار دچار مشکل و گیر کردن شده باشد، توسط این گزینه، آن را می بندیم.
- **Finder**: توسط گزینه ی Prefrences و در تب General می توان تنظیمات Desktop را انجام داد.
- محل نمایش search، ساعت، زبان، وضعیت WiFi و ... در سمت راست، که با نگه داشتن دکمه ی Command و drag کردن، می توان این option ها را جابجا کرد.

منوی File:

- در Windows، پنجره ای وجود دارد به نام File Explorer که به Document ها و Drive ها هدایت می شود.
- نسخه ی مک برای File Explorer، به نام Finder Window وجود دارد.
- یک قابلیت Finder Window این است که مثل مرورگر مثلاً Firefox، می تواند پنجره های دیگری را به عنوان تب های داخل خودش، اضافه کند.
- در منوی Finder، توسط گزینه ی Prefrences و در تب General می توان صفحه ی پیشفرض Finder ها را تنظیم کرد.
- به سادگی می توان new folder ایجاد کرد و با drag کردن می توان Folder ها را به side bar نیز پیوند کرد.
- در Windows نواری به نام Address Bar وجود دارد، اما در mac برای پیدا کردن آدرس یک پنجره، Command یا Control را نگه داشته و در بالای آن پنجره روی نام آن پنجره کلیک می کنیم.

منوی View:

- معمولاً چند گزینه ی اول در این منو را به صورت یک آیکون کوچک در تمام پنجره هایی که باز می کنیم، مشاهده خواهیم کرد.
- اما فعال سازی گزینه های زیر، خالی از لطف نیست:
  - **Clean up by** < Name یا Size یا Data modified
  - **Show Path bar**
  - **Show Status Bar**
  - **Show View Options**

منوی Go:

- همانطور که در Windows گزینه ی مهمی به نام My Computer یا This PC وجود دارد، در اینجا معادل آن Computer است.
- Computer شامل فضای حافظه و فضای مرتبط با شبکه است.
- هنگام باز کردن منوی Go، اگر کلید option را نگه داریم، گزینه ی Library نیز در لیست آن ظاهر می شود.
- می دانیم که در Windows برای مشاهده ی یک سری ویژگی های یک فایل؛ با کلیک راست روی آن، وارد Properties می شویم، که این گزینه در mac با نام Get Info وجود دارد.

❖ صفحه ی عریض Desktop: درست مثل دسکتاپ Windows، در اینجا می توان با راست کلیک کردن، پوشه‌های جدید ایجاد کرد و با کشیدن فایل‌ها، می‌توان آنها را مرتب کرد.

❖ Dock: یا همان نوار پایین که شامل تعدادی Icon می باشد.

Dock به دو بخش تقسیم می‌شود. یک بخش که مربوط به میانبرهای Application هاست و بخش دیگر که پوشه‌های سنجاق شده و پنجره‌های کوچک شده را در بر می‌گیرد.

- می‌توان Dock را طوری تنظیم کرد که در پایین، چپ یا راستِ Desktop قرار بگیرد.
- برای تنظیم dock یا می توان بر روی خط کوچکی که آن را به دو بخش تقسیم می کند، کلیک راست کرد و یا به مسیر زیر رفت:

Apple menu < System Prefrences < Dock

- معمولاً اولین گزینه از سمت چپ، گزینه ی **Finder** است که کار **New Finder Window** را انجام می دهد.
- **App** هایی که در **Dock**، پیوست نشده باشند، در زمان اجرا، آیکون آنها، در **Dock** نمایش داده می شود.
- با کشیدن و رها کردن هر **Icon** به خارج از **Dock**، آن گزینه از **Dock** حذف خواهد شد.
- اگر فایل یک **Application** را کشیده و در **Dock** رها کنیم، یک **Shortcut** از آن در **Dock** ایجاد خواهد شد.

❖ **Activity Monitor**:

برای مشاهده ی میزان مصرف **CPU** و **RAM** و برق و حافظه و شبکه، از این کنسول در **mac** استفاده می شود، که در مسیر زیر قرار دارد:

Launchpad > Other > Activity Monitor

❖ **Applications**:

همانطور که می دانیم در ویندوز، وقتی روی دکمه ی **Start** (**windows**) در سمت چپ کلیک می کنیم، در فهرست ظاهر شده، فهرست بالابلندی وجود دارد به نام **All Programs** .

در **mac** برای مشاهده ی اینچنین منویی که همه ی نرم افزارهای نصب شده روی سیستم عامل را نشان دهد، وارد آبجکت هارد دیسکی که ویندوز روی آن نصب شده است، می شویم. می بینیم که چهار پوشه وجود دارند که اولین، پوشه ی **Application** است.

پس این پوشه را با **drag** کردن، به سمت راست نوار **Dock** می کشیم.

حال روی آیکونِ آن که به **dock** اضافه شده است کلیک راست کرده و مثلاً **list** را انتخاب می کنیم.

❖ **Work on files**:

در **mac** هم می توان یک فایل را **copy** کرد و هم می توان **paste** کرد؛ اما نمی توان **cut** کرد، بلکه برای جابجایی کامل یک فایل، ابتدا آن را کپی می کنیم، سپس در مقصد، کلیک راست کرده و **move item here** را می زنیم؛ که مشابه با **Cut** خواهد بود.

اما اگر با کلیک راست، این گزینه ظاهر نشد، در همان حالت راست کلیک، دکمه ی **option** را نگه می داریم تا ظاهر شود.

Search:

ابزاری که در **mac** جهت جستجو بکار می رود، **Spotlight** نام دارد که ابزاری بسیار قدرتمند ست.

در نوار ابزار بالا و با علامت ذره بین قابل دسترسی است.

Spotlight جستجو را بر اساس تمام فایل های موجود و قابل دسترسی در تمام فضای ذخیره سازی داخلی و آنلاین و محتوای ایمیل ها و ... انجام می دهد.

اگر بخواهیم جستجو را بر اساس یک مکان یا پوشه ی خاص انجام دهد، وارد **System Preferences** و گزینه ی **Spotlight** شده و به تب **Privacy** می رویم و توسط گزینه ی **+** ، محل جستجوی موردنظر را انتخاب می کنیم.

:System Preferences

این بخش از **mac** در حقیقت همان **Control Panel** موجود در **Windows** است.

می بینیم که شامل چهار بخش کلی است:

- **Personal** : اگر تغییری در تنظیمات مربوط به گزینه های این بخش بدهیم، فقط برای **User** ای که اکنون با آن **login** شده ایم، صورت خواهد گرفت.
- **Hardware**
- **Internet and Wireless**
- **System**

❖ **:Startup programs**

پس از مدتی که نرم افزارها و ابزارهایی را نصب و راه اندازی کردیم، می بینیم که برخی از آنها، فوری پس از روشن کردن و ورود به سیستم، به طور خودکار، شروع به کار می کنند.

برای مشاهده و یا غیرفعال کردن این اجرای خودکار آنها، به **System Preferences** و **Users & Groups** رفته و **User** ای که با آن **login** کرده ایم را انتخاب کرده و در سمت راست، وارد تب **Login Items** می شویم.

:Network

مدیریت کلیه ی تنظیمات شبکه در mac در مسیر زیر قرار دارد:

System Preferences > Network

- در کادر سمت چپ، کارت های شبکه را مشاهده می کنیم. (شبکه های کابلی [Ethernet]، WiFi و ...)
- معادل cmd در سیستم عامل mac، کنسول Terminal است که مشابه Terminal موجود در Linux است.

:Join to a Domain ➢

به مسیر زیر می رویم:

System Preferences > Users & Groups

- روی Login Options کلیک می کنیم.
- قفل پنجره را باز می کنیم. (Click the lock to make changes)
- روی دکمه ی Join مقابل Network Account Server کلیک می کنیم.
- روی دکمه ی Open Directory Utilities کلیک می کنیم.
- قفل پنجره را باز می کنیم. (Click the lock to make changes)
- Active Directory را انتخاب می کنیم.
- روی آیکون کوچک مداد (Edit) در پایین کلیک می کنیم.
- نام Domain موردنظر (مثلاً payamavar.local) و نام خود این کامپیوتر (Hostname) را وارد می کنیم.
- اگر تمایل به تنظیمات اضافه داشته باشیم، می توانیم روی دکمه ی مثلث افقی کوچک در پایین این پنجره کلیک کنیم.
- وارد تب Administrative شده و ..Prefer this D را فعال کرده و آدرس FQDN مربوط به سیستم DC را درج می کنیم.
- اگر بخواهیم مجوزهای مدیریتی به این سیستم بدهیم، گزینه ی Allow administration by را فعال کرده و نام Group های موردنظر موجود در Domain را درج و اضافه می کنیم؛ و OK می کنیم.
- Bind را می زنیم.
- مشخصات حساب Administrator در Domain را وارد می کنیم و OK.
- باید پیامی موفقیت آمیز، مشابه PC is joined to the domain ظاهر شود و دکمه ی Bind به Unbind تبدیل شود.
- حال اگر به پنجره ی Accounts و گزینه ی Login Options برگردیم، می بینیم که مقابل Network Account Server نام Domain با یک چراغ سبز ظاهر شده است.
- حال یک بار سیستم را Restart می کنیم تا به صفحه ی Login Screen برسیم.
- روی گزینه ی other کلیک می کنیم.
- حال با مشخصات یک User که در Domain (Active Directory) است، وارد می شویم.
- برای دسترسی به فایل های Share شده در Domain، باید map drive ایجاد کنیم.
- پس از منوی Finder، روی Conect to Server کلیک کرده و در پنجره ی باز شده، آدرس فایل های مقصد را به صورت زیر در Server adress درج کرده و Connect را می زنیم:

Smb://servername/...

:Mac maintenance

➢ :Apple ID

همانطور که اخیراً برای استفاده از برخی ابزارها و سرویس های ویندوز مثل One drive و ... ، نیاز به ایجاد یک Account در سایت Microsoft می باشیم. در mac هم جهت استفاده از برخی ابزارهای آن مثل App Store ، iTunes و ... ، نیاز به داشتن یک Account در سایت Apple خواهیم داشت، که به این حساب، Apple ID گفته می شود.

Apple به ازای هر AppleID پنج گیگابایت فضای ذخیره‌سازی آنلاین در اختیار قرار می‌دهد و تفاوتی ندارد که آیفون خریده باشید، Apple TV تهیه کرده باشید یا یک MacBook جدید باشد.

این فضای ذخیره سازی را می توان افزایش داد که حجم های بالاتر، هزینه های ماهیانه ی بیشتری خواهند داشت.

- کنسول یا ابزار مدیریت این فضای ذخیره سازی، iCloud می باشد.

➢ :Update

آن را به روز نگه می داریم.

برای دریافت Update های کلی سیستم عامل و همچنین نسخه‌های جدید نرم‌افزارهای Apple، تنها کافی ست App Store را باز کرده و وارد زبانه‌ی Updates شویم.

➢ :Backup

از فایل های موجود، نسخه پشتیبان تهیه می کنیم.

راه حل Apple برای پشتیبان‌گیری، یک روش خودکار و توسط Time Machine می باشد.

برای این کار نیاز به یک external storage یا یک محل مشخص شده در شبکه خواهیم داشت.

- حافظه ی خارجی را به mac متصل می کنیم.
- حال از طریق System Preferences به Time Machine می رویم.
- گزینه ی Select Backup Disk را زده و درایو یا دیسک موردنظر جهت Backup را انتخاب می کنیم.
- پس شروع به انجام یک پشتیبانگیری کامل می کند.
- حال، هر زمان که این درایو را به mac متصل کنید، Time Machine اقدام به تهیه‌ی یک Backup خواهد کرد.
- البته هر بار از همه چیز Backup نمی گیرد.
- تنها هر بار سعی می‌کند از تغییرات به وجود آمده پشتیبان بگیرد.
  - هر گاه درایو مورد نظر پر شود، Backup های قدیمی‌تر حذف می‌شوند!
  - هر زمان که درایو خود را متصل نمایید، امکان مشاهده‌ی Backup ها را خواهید داشت.

➢ :Storage

همیشه یک مقدار فضای خالی، حدود 10 GB را خالی نگه می داریم و هیچگاه فضای ذخیره سازی سیستم عامل را کاملاً پُر نمی کنیم.

- برای کنترل، تنظیم و مدیریت Hard Disk ها، حافظه های جانبی و DVD drive ها و ... ، به مسیر و کنسول زیر می رویم:

Launchpad > Other > Disk Utility

- برای کنترل و مدیریت کلیه ی Storage ها به مسیر زیر می رویم:

Apple menu > About this mac > storage > manage

  - اگر Empty Trash Automatically روشن کنیم، هر سی روز یکبار، محتویات سطل زباله بطورخودکار حذف می شوند.
  - توسط گزینه ی Reduce Clutter و دکمه ی Review Files می توانیم لیستی از بزرگترین فایل‌ها و همچنین فایل های کمتر استفاده شده را ببینیم؛ و می توانیم موارد دلخواه را حذف کنیم.

Software:

- همانطور که می دانیم هرگاه که یک پنجره یا برنامه را باز می کنیم، نوار منوی بالای mac نیز تغییر کرده و مطابق با آن پنجره یا برنامه می شود.
- همانطور که می دانیم، هر نرم افزار نیز، بطور جداگانه نیاز به تنظیمات خاص خودش دارد.
- برای ورود به تنظیمات یک نرم افزار، ابتدا آن را باز کرده و سپس از منوی بالا، روی نام نرم افزار که جایگزین Finder در منو شده است، کلیک کرده و گزینه ی Preferences را می زنیم.

نصب نرم افزار:

- در حقیقت به طورکلی برای استفاده از خیلی از امکانات موجود در mac باید یک Apple ID ایجاد و فعال کرده باشیم، در مورد کنسول App Store هم به همین شکل خواهد بود، و بدون داشتن Apple ID هیچ نرم افزاری را نمی توان دریافت و نصب کرد، حتی نرم افزارهای رایگان را!!

- روش دیگر جهت نصب نرم افزار این است که فایل نصب نرم افزارها را به هر شکلی به جز App Store تهیه و در سیستم نصب کرد. که بهتر است فقط نرم افزارهای Crack شده و یا نرم افزارهایی که می توانیم نیازی به update های آنها نداشته باشیم را به این روش نصب کنیم!
  - ✓ فرمت فایل های نصبی در ویندوز، exe می باشد و در مک، dmg می باشد.
  - ✓ در این روش، ابتدا باید در System Preferences به System and Security رفته و در تب General گزینه ی Allow apps downloaded را تنظیم کنیم.

پس از باز کردن پوشه ی نصب نرم افزار، فایل dmg را باز می کنیم؛ سپس در صفحه ی باز شده، فایل یا آبجکت نرم افزار را با drag کردن، به پوشه ی Applications می بریم.

- اگر پیغام خطایی مشابه can't be opened. Zou should move it to the trash ظاهر شد، به جهت باز بودن Gate Keeper است، پس ابتدا Terminal را باز کرده (توسط Admin user) و دستور زیر را وارد می کنیم:

```
sudo spctl –master-disable
```

پسورد admin را وارد می کنیم و تمام!

نکته: البته گاهی، این فایل یا آجکت نرم افزار، نوعی Installer است (از نامش هم پیداست)، پس روی خود فایل باید دابل کلیک کرد و نصب را از این طریق ادامه داد.

- اگر نرم افزار دارای یک فایل crack یا Keygen باشد، آن را در همین صفحه باز کرده و open را زده و فایل خود نرم افزار را انتخاب می کنیم و save .

سپس کافی ست به Launchpad برویم تا نرم افزار نصب شده را مشاهده کنیم.

نکته: اگر Gate Keeper را توسط دستور بالا، غیرفعال کردیم، در پایان پس از راه اندازی کامل نرم افزار، بهتر است که Gate keeper را به صورت زیر دوباره فعال کنیم:

```
sudo spctl –master-enable
```

- **Safari:**

برای افزودن یک **page** به عنوان **Bookmark** در نوار بالای مرورگر، در سمت راست، توسط دکمه ی **share**، گزینه ی **Add Bookmark** را زده و آن را به عنوان **Favorite** انتخاب می کنیم.

- **AirPort:**

جهت ایجاد ارتباط (شبکه) میان دستگاه های شرکت **Apple** استفاده می شود.

- **Parallel Desktop:**

معادل **Vmware** و **Virtual Box** می باشد.
توسط این برنامه، که بطورپیشفرض بر روی **mac** وجود ندارد و باید آنها تهیه و نصب کرد، می توان سیستم عامل های دیگری را به صورت مجازی راه اندازی و همزمان با سیستم **mac**، استفاده کرد.

- **Keychain:**

✓ در سیستم عامل **mac**، از ابزار **Keychain** جهت کنترل و ذخیره سازی **Username** و **Password** ها استفاده می شود. درست مثل **Credential manager** در **Windows**.

:Terminal

Ping کردن در **Terminal** مشابه با **cmd** در ویندوز است، اما در اینجا ارسال بسته ها قطع نمی شود تا اینکه خودمان آن را قطع کنیم. (**Ctrl+C**)
و یا به شکل مقابل می توان تعداد بسته ها را مشخص کرد:

ping -c 5 192.168.0.1

درحقیقت، کار با **Terminal** در سیستم عامل‌های **Linux**، **Unix** و **Macintosh** مشابه می باشد.

عملکرد	توضیح	دستور
دریافت تنظیمات **IP**		Ifconfig
دریافت **IP v4**	Find IPv4	Ipconfig getifaddr en0
نمایش مسیر ذخیره پروژه یا دایرکتوری(**Directory**)	Print Working Directory	pwd
نام شبکه رایانه	Computer’s Network Name	hostname
ایجاد دایرکتوری	Make Directory	mkdir
تغییر دایرکتوری	Change Directory	cd
فهرست کردن دایرکتوری	List Directory	ls
یافتن فایل‌های مورد نظر	Find Files	find
حذف کردن دایرکتوری	Remove Directory	rmdir
نمایش محتویات فایل با اسکرول کردن(**Scroll**)	Page Through File	less
کپی کردن فایل یا دایرکتوری	Copy File or Directory	cp
جابجایی فایل یا دایرکتوری	Move File or Directory	mv
ذخیره دایرکتوری فعلی در حافظه رایانه	Push Directory	pushd
بازگردانی دایرکتوری ذخیره شده	Pop Directory	popd
پیدا کردن موارد مختلف در درون یک فایل	Find Things Inside Files	grep
اجرای آرگومان‌ها	Execute Arguments	xarg
نمایش تمامی قسمت‌های یک فایل	Print the Whole File	cat
نمایش متغیرهای محیطی	Look at Environment	env
ذخیره/تنظیم یک متغیر محیطی جدید	Export/Set a New Environment Variable	export
نمایش برخی از آرگومان‌ها	Print Some Arguments	echo
خواندن یک صفحه راهنما	Read a Manual Page	man
یافتن صفحه راهنمای مناسب	Find What Man Page Is Appropriate	apropos
تغییر مالکیت گروه یک فایل و یا یک پوشه	Change Ownership	chown
تغییر و محدود کردن مجوز دسترسی	Change Permission Modifiers	chmod
خروج از محیط کدنویسی	Exit Shell	exit
به دست آوردن مجوزهای دسترسی **Root**، این دستور می‌تواند باعث آسیب‌پذیری سیستم شود!	Danger! Become Super User Root Danger	sudo

:Shortcuts

Opens a new Finder Window	**Command + N**
Closes a Finder Window	**Command + W**
Exit from a Software/Application	**Command + Q**
Runs the *Force Quit*	**Command + Option + Esc**
Creates a New Folder	**Command + Shift + N**
Rename a Folder	**Enter**
Open a Folder	**Command + O**
Shows View Options	**Command + J**
Opens Computer	**Command + Shift + C**
Move to trash function	**Command + Back space**
Empties the Trash	**Command + Shift + Back space**
Get Info	**Command + i**
Select all	**Command + A**
Copy file or text	**Command + C**
Paste file or text	**Command + V**
Cut text	**Command + X**
New Tab In Safari	**Command + T**
Close Tab in Safari	**Command + W**
Undo an action	**Command + Z**
Search (Spotlight)	**Command + Space**
Makes a screenshot	**Command + Shift + 3**
Change between input languages	**Ctrl + Space**
Change between open windows	**Ctrl + UP arrow**
Change between current Desktops	**Ctrl + Right/Left arrow**

:Troubleshooting

در سیستم های mac دو نوع حافظه وجود دارند:

- **PRAM** (Parameter Random Access Memory)
- **SMC** (System Management Controller)

برخی از عوامل بالانیامدن سیستم عامل mac، تنها با Restart کردن PRAM و یا SMC حل می‌شوند.

این دو حافظه، نقش مهمی در اجرای سالم mac دارند و کارهایی نظیر مدیریت زمان و تاریخ و یا کنترل عناصر فیزیکی، مثل فن و چراغ‌های LED را انجام می‌دهند.

اگر مشکلاتی مثل:

- کار نکردن صدای mac،
- عدم موفقیت در پیدا کردن Boot partition
- رفتار عجیب Keyboard یا mouse، تغییر Resolution تصویر یا خاموش شدن آهسته‌ی mac،

وجود داشته باشند، ریست کردن PRAM می‌تواند راه حل مناسبی باشد.

اگر مشکلاتی مثل:

- رفتار غیر عادی در فن یا چراغ‌های LED یا چراغ Power بر روی شارژر
- اگر با باز کردن دربِ mac، دیگر روشن نمی‌شد،
- مشکل WiFi وجود داشته باشد،
- mac پیش از حد آهسته کار می کند،

وجود داشته باشند، ممکن است با ریست کردنSMC ، برطرف شوند.

بر اساس مدل mac، ریست کردن «PRAM» و «SMC» می‌تواند راه متفاوتی داشته باشد که با کمی جست‌وجو می‌توان روش آن را پیدا کرد.

➢ :It doesn't show the Storage drive

فرض کنید یک external Hard را به سیستم متصل کرده اید، اما Icon آن در Desktop اضافه نشده است.

به منوی Finder رفته و وارد Prefrences شده و در تب General یکبار گزینه ی External disks را غیرفعال و دوباره فعال می کنیم.

➢ :Mac doesn't boot

فرض کنید سیستم پس از boot شدن، به جای رفتن به محیط login screen، به یک صفحه ی خاکستری رنگ می رود!

پس باید آن را در safe mode راه اندازی کنیم، که سیستم بطور خودکار، مشکلات موجود را بررسی و در صورت امکان رفع کند.

- پس سیستم را Restart کرده و کلید shift را نگه می داریم.
- حال باید منتظر ماند تا به صفحه ی login برود، که ممکن است چند دقیقه طول بکشد.
- پس از ورود به login screen، می توان دکمه را رها کرد.

Ticket System:

به نرم افزاری که جهت مدیریت و کنترل ارتباط با مشتری یا همکاران باشد، **CRM** یا **C**ustomer **R**elationship **M**anagement گفته می شود.

یکی از بهترین راهکارهای نرم افزاری جهت مکاتبات اداری، راه اندازی نرم افزارهایی مشابه با شبکه های اجتماعی عمومی هستند که هر مساله یا اشکال یا کمبود یا درخواست(Query) از هر یک از بخش ها یا پرسنل شرکت و یا از هریک از مشتری ها از خارج از شرکت، در قالب یک درخواست (**Request**) مشابه با **Post** های کاربران در شبکه های اجتماعی، در این نرم افزارها ارسال می شوند.

نام عمومی که به این گونه نرم افزارها نسبت می دهند، **Ticket System** یا **Ticketing Software** می باشد.

درحقیقت به این جهت که به هریک از درخواست ها و مکاتبات در نرم افزار **CRM**، یک **Ticket** گفته می شود، به این نرم افزارها، سیستم **Ticket** گفته می شود.

نرم افزارهای زیادی در زمینه ی **ticketing** وجود دارند، اما برخی از معروف ترین ها عبارتند از:

- **Jira**
- **Spiceworks**
- **Servicenow**

مزایای Ticket System:

- افزایش تولید و باروری
- کاهش هزینه ها
- افزایش سطح سرویس دهی
- بهبود رابطه با مشتری
- **Centralization** : تمامی **Customer communication** های شرکت (ارتباطات با مشتری)، به شکل متمرکزتری کنترل می شوند.
- **Systematic and organized** : هر تکنسین بر اساس تخصص و مهارتش، **Ticket** مخصوص خودش را رسیدگی خواهد کرد.
- **Prioritization** : درخواست **Support** مشتری ها را بر اساس مقادیر زیر، اولویت بندی می کنیم:
  - میزان بحرانی بودن **Ticket**
  - اهمیت شخص درخواست دهنده
- **Improvement of internal Communications** : روابط میان پرسنل شرکت با یکدیگر نیز بهبود می یابد.

انواع Ticketing System :

- **Cloud based** :
- **On-premises** (در محل):
- **Enterprise** :
- **Open-Source** :

بخش های اصلی در یک Ticketing System :

- **Site** ها و **User** هایی که نیاز به **Support** خواهند داشت.
- **Channel** هایی که درخواست های **User** ها را دریافت می کنند: **Email**، **Phone**، **Web Portal**، **Chat** و ... .

نوشته ی
پیام اوَروند
تابستان 2021 - 1400

- Payam_Avar@yahoo.com
- @payam.avarwand